1. Barracuda Backup - Overview 4
1.1 What's New in Barracuda Backup 4
1.2 Deployment Options 6
1.2.1 Barracuda Backup Deployment Template 6
1.2.2 Site-to-Site Deployment 14
1.2.2.1 Configuring Replication 21
1.2.3 Site-to-Cloud Deployment 22
1.2.4 Barracuda Cloud Storage Deployment Overview 27
1.3 Getting Started 27
1.3.1 Step 1: How to Install the Barracuda Backup Server 27
1.3.2 Step 2: How to Configure Barracuda Backup 28
1.3.3 Step 3: How to Configure Backups 30
1.3.4 Step 4: Data Backup Tasks 33
1.4 Web Interface 36
1.4.1 STATUS Page 37
1.4.1.1 How to Monitor Backup Status 41
1.4.1.2 How to Unlink a Barracuda Backup Server 41
1.4.1.3 Task Messages 42
1.4.2 BACKUP Page 43
1.4.2.1 Understanding Source-Based Deduplication 45
1.4.2.2 Backing Up Data Sources 46
1.4.2.2.1 Microsoft Exchange Server and Exchange Server DAG 46
1.4.2.2.2 Microsoft Hyper-V 65
1.4.2.2.3 Microsoft SQL Server 69
1.4.2.2.4 VMware 74
1.4.2.2.5 How to Back Up Microsoft Active Directory 78
1.4.2.2.6 How to Back Up and Restore a Microsoft SharePoint SQL Database 79
1.4.2.2.7 Understanding IBM Domino Server Backup 84
1.4.2.2.8 How to Configure GroupWise Message-Level Backups 86
1.4.2.2.9 How to Set Up a Root Account to Back Up Macintosh OS X 89
1.4.2.2.10 How to Back Up Linux/UNIX Data Using SSHFS 91
1.4.2.2.11 Understanding Changed Block Tracking on Virtual Machines 94
1.4.2.2.12 How to Enable Changed Block Tracking through the Barracuda Backup Web Interface 95
1.4.2.2.13 How to Back Up Network Addressable Storage - NAS 98
1.4.2.2.14 How to Back Up FirstClass Mail 99
1.4.2.2.15 How to Back Up NFS Mounts with the Barracuda Backup Agent (Linux) 100
1.4.2.2.16 How to Back Up NSS Mounts with the Barracuda Backup Agent (Linux) 101
1.4.2.3 Replication Page 101
1.4.2.3.1 Configuring a Replication Destination 102
1.4.2.3.2 How to Temporarily Disable a Destination 104
1.4.2.3.3 How to Manage the Data Queue 104
1.4.2.4 Schedules Page 105
1.4.2.5 Rate Limit Page 109
1.4.2.6 Exclusions Page 110
1.4.2.7 Retention Policies Page 111
1.4.2.7.1 Understanding Retention Policies 111
1.4.2.7.2 How to Create Retention Policies 113
1.4.2.7.3 Understanding Barracuda Offsite Vaulting 113
1.4.2.7.4 Creating Effective Retention Policies 114
1.4.2.7.5 Retention Policy Example 116
1.4.2.8 Watched Files Page 117
1.4.3 RESTORE Page 117
1.4.3.1 VMware Server Recovery and Restoration 118
1.4.3.1.1 How to Restore a Virtual Machine to its Original Location 118
1.4.3.1.2 How to Restore a Virtual Machine to a Different Host Protected by Barracuda Backup 119
1.4.3.1.3 How to Restore a Virtual Machine to an Alternate VMware Host not available through the Barracuda Backup Service 119
1.4.3.1.4 VMware Data Recovery Licenses 120
1.4.3.1.5 How to Restore VMware Guest Systems Using Barracuda LiveBoot 120
1.4.3.2 Microsoft Exchange Server Recovery and Restoration 126
1.4.3.2.1 How to Restore a Microsoft Exchange 2013 Server Database to a Recovery Storage Group 126

1.4.3.2.2 How to Restore a Microsoft Exchange 2010 Server by Overwriting an Existing Database . . . 128
1.4.3.2.3 How to Restore a Microsoft Exchange 2010 Server to a Recovery Database . . . 131
1.4.3.2.4 How to Restore a Microsoft Exchange 2007 Database . . . 134
1.4.3.2.5 How to Restore a Microsoft Exchange 2003 Database by Overwriting Existing Database . . . 145
1.4.3.2.6 How to Restore a Microsoft Exchange 2003 Database using a Recovery Storage Group . . . 148
1.4.3.3 Microsoft SQL Server Database Recovery and Restoration . . . 159
1.4.3.3.1 How to Restore a Microsoft SQL Database . . . 160
1.4.3.3.2 How to Restore a SQL Server 2008 Master Database . . . 161
1.4.3.3.3 How to Restore a Microsoft SQL Database to a Point-in-Time . . . 163
1.4.3.3.4 How to Restore a Microsoft SQL Server Database to a Flat File . . . 169
1.4.3.4 Microsoft Hyper-V Recovery and Restoration . . . 170
1.4.3.4.1 How to Restore a Microsoft Hyper-V 2012 to its Original Location . . . 171
1.4.3.4.2 How to Restore a Microsoft Hyper-V Virtual Machine . . . 171
1.4.3.5 Microsoft Windows Server Active Directory . . . 175
1.4.3.5.1 How to Restore a Microsoft Server 2012 Active Directory Object from the Active Directory Recycle Bin . . . 175
1.4.3.5.2 How to Enable Active Directory Recycle Bin on Windows Server 2012 . . . 177
1.4.3.5.3 How to Restore a Microsoft Server 2008 R2 Active Directory Object from the Active Directory Recycle Bin . . . 178
1.4.3.5.4 How to Enable Active Directory Recycle Bin on Windows Server 2008 R2 . . . 179
1.4.3.6 Barracuda LiveBoot in the Cloud . . . 181
1.4.3.6.1 Understanding Cloud LiveBoot . . . 181
1.4.3.6.2 How to Use Barracuda LiveBoot in the Cloud . . . 182
1.4.3.6.3 How to vMotion a LiveBooted Virtual Machine from the Barracuda Backup Server . . . 188
1.4.3.7 Barracuda copy.com . . . 194
1.4.3.7.1 How to Restore to a copy.com Account . . . 194
1.4.3.7.2 How to Share and View Files Using copy.com . . . 196
1.4.3.8 Restore Browser . . . 197
1.4.3.8.1 Understanding Restore Browser . . . 197
1.4.3.8.2 How to Search for Items Using the Restore Browser . . . 197
1.4.3.8.3 How to Restore Data Using the Restore Browser . . . 199
1.4.3.9 How to Restore from Local and Offsite Backups . . . 201
1.4.3.10 How to Recover Backed Up Data . . . 201
1.4.3.10.1 Example - Restore Data Using the Local Web Interface . . . 204
1.4.3.11 How to Restore from a Replication Destination . . . 206
1.4.3.12 How to Restore SharePoint Objects Using Kroll Ontrack . . . 208
1.4.3.13 How to Restore a Microsoft Windows Server 2003 Domain Controller . . . 215
1.4.3.14 How to Restore Windows System State . . . 216
1.4.3.14.1 How to Restore Windows Server 2003 Domain Controller System State . . . 216
1.4.3.14.2 How to Restore Windows Server 2008 Domain Controller System State . . . 220
1.4.3.15 How to Restore Exchange and GroupWise Messages . . . 226
1.4.3.16 How to Restore a Windows System to Bare Metal . . . 226
1.4.3.17 How to Restore a Linux Server Using Bare Metal Restore . . . 233
1.4.3.18 How to Restore Data with FTPES . . . 238
1.4.3.19 Legacy Firmware Recovery and Restoration Options . . . 239
1.4.3.19.1 How to Use Windows Explorer and WebDAV . . . 239
1.4.3.19.2 How to Restore Data with an FTP Client . . . 239
1.4.3.19.3 Barracuda Restore for Windows . . . 240
1.4.4 REPORTS Page . . . 250
1.4.5 SYSTEM Page . . . 252
1.4.5.1 Firmware Page . . . 253
1.4.5.2 BBS Settings Page . . . 254
1.4.5.3 Software Downloads Page . . . 254
1.4.5.4 Advanced Graphs Page . . . 254
1.4.6 ADMIN Page . . . 258
1.4.6.1 Users Page . . . 259
1.4.6.1.1 Managing Your Account . . . 260
1.4.6.1.2 Managing User Access . . . 261
1.4.6.1.3 Product Entitlements . . . 261
1.4.6.2 Email Notifications Page . . . 263
1.4.6.3 Display Groups Page . . . 263
1.4.6.4 Documentation Page . . . 264
1.4.6.5 Link a Barracuda Backup Server Page . . . 264

- 1.4.6.5.1 How to Link a Barracuda Backup Server as a User or Reseller . . . 264

1.5 Security . . . 268
- 1.5.1 Backup Security and Site-to-Site Replication . . . 268
- 1.5.2 Barracuda Cloud Storage Standards and Protection . . . 268
- 1.5.3 Policy-Based Security . . . 269
- 1.5.4 How to Secure Your Barracuda Backup Server . . . 269

1.6 System Management . . . 270
- 1.6.1 Barracuda Backup Replacement and Data Migration . . . 270
- 1.6.2 Replacing a Failed Barracuda Backup Server . . . 272
- 1.6.3 How to Shut Down a Barracuda Backup Server . . . 272
- 1.6.4 How to Wipe a Barracuda Backup Server . . . 272
- 1.6.5 Barracuda Backup Server Panel Indicators, Ports, and Connectors . . . 273
- 1.6.6 Barracuda Backup Server Hardware Specifications . . . 280
- 1.6.7 How to Physically Install the Barracuda Backup Server . . . 282

1.7 Troubleshooting and Error Messages . . . 286
- 1.7.1 Understanding Why the Barracuda Backup Agent Moves to a New Volume . . . 287
- 1.7.2 Understanding Why Data is not Replicating to an Offsite Barracuda Backup Location . . . 287
- 1.7.3 How to Troubleshoot Using the Barracuda Backup Agent (Windows) Log File . . . 288
- 1.7.4 How to Resolve Low Disk Space . . . 289
- 1.7.5 How to Change the Barracuda Backup Agent Port Number . . . 290
- 1.7.6 How to Change the Barracuda Linux Backup Agent Port Number . . . 291
- 1.7.7 How to Change the SQL Recovery Model . . . 292
- 1.7.8 How to Resolve Microsoft Exchange 2010 Large Message Restore Errors . . . 293
- 1.7.9 How to Resolve Snapshot Backup Errors . . . 302
- 1.7.10 Resolving "Agent database moved to different location" Warning . . . 305
- 1.7.11 Resolving "Error Creating Snapshot" Error During ESX/ESXi Virtual Machine Backup . . . 305
- 1.7.12 Resolving "Error Reading Object" Error During ESX or ESXi Virtual Machine Backup . . . 306
- 1.7.13 Resolving "Error Removing Snapshot" Error During ESX/ESXi Virtual Machine Backup . . . 306
- 1.7.14 Resolving "Failed to connect to backup agent software" Error . . . 307
- 1.7.15 Resolving "File System Snapshot was Released" Error . . . 308
- 1.7.16 Resolving "Incremental backups cannot be performed while circular logging is enabled" Error . . . 311
- 1.7.17 Resolving “An error occurred during agent backup initialization" Error . . . 312
- 1.7.18 Resolving "Unable to back up virtual machines with independent disks" Error . . . 314
- 1.7.19 Resolving "VMDK is larger than the maximum size supported by datastore" Error . . . 314
- 1.7.20 Resolving "Error backing up selected object" Error . . . 317
- 1.7.21 Resolving "An unknown OS error occurred" Error . . . 318
- 1.7.22 Resolve the "Failure while using USN journal" Error . . . 320
- 1.7.23 Monitoring Windows System Performance During Backup . . . 321
- 1.7.24 How to Increase Backup Performance . . . 322

1.8 Agents and Tools . . . 323
- 1.8.1 Barracuda Backup Agent (Windows) . . . 323
  - 1.8.1.1 How to Install and Use the Barracuda Backup Agent (Windows) . . . 323
  - 1.8.1.2 How to Silently Install the Barracuda Backup Agent (Windows) . . . 325
  - 1.8.1.3 Understanding the Barracuda Backup Agent (Windows) File Structure . . . 326
  - 1.8.1.4 How to Manually Move the Barracuda Backup Agent (Windows) Database to an Alternate Location . . . 327
- 1.8.2 Barracuda Backup Agent (Linux) . . . 329
  - 1.8.2.1 How to Install and Use the Barracuda Backup Agent (Linux) . . . 329
  - 1.8.2.2 How to Manually Move the Barracuda Backup Agent (Linux) Database to an Alternate Location . . . 331
- 1.8.3 How to Edit Network Settings through the Barracuda Console . . . 332

1.9 Hardware Compliance . . . 333

1.10 Limited Warranty and License . . . 334

Barracuda Backup - Overview

The Barracuda Backup is an affordable solution for onsite and remote data storage and access. Quickly and securely store data in multiple offsite locations. Barracuda Backup removes duplicate data inline at the block level to reduce traditional backup storage requirements up to 25 times, while reducing backup windows and bandwidth requirements.

Where to Start

Download the Barracuda Backup Service Quick Start Guide including English, German, and Japanese translations.

For detailed installation and configuration steps, start here:

- Step 1: How to Install the Barracuda Backup Server
- Step 2: How to Configure Barracuda Backup
- Step 3: How to Configure Backups
- Step 4: Data Backup Tasks

Key Features

- Deduplication - Barracuda removes duplicate data both inline and across all sources via block and file-level deduplication.
- Data Sources - Choose the method for backing up data based on the type of data and data source.
- Recovery and Restoration - Restore data from the local Barracuda Backup Server, from a remote Barracuda Backup Server that has been used to replicate that system, or from Barracuda Cloud Storage.
- Barracuda LiveBoot - Use Barracuda LiveBoot to boot VMware virtual guest systems in the Barracuda Cloud. LiveBoot in the cloud is useful as a sandbox for testing purposes.
- copy.com Integration - Share and back up folders and files backed up in the cloud via Copy.
- Backup Analytics - View a detailed list of large items by source or file name in the **REPORTS > Large Items** page.

Web Interface

- STATUS Page - View an overview of the performance and health of your Barracuda Backup.
- BACKUP Page - Set up and manage data source backup.
- RESTORE Page - Restore data from the local Barracuda Backup Server, from a remote Barracuda Backup Server that has been used to replicate that system, or from the Barracuda Cloud Storage.
- REPORTS Page - View detailed reports for each backup that is run.
- SYSTEM Page - Manage the Barracuda Backup firmware version and settings, and access software downloads.
- ADMIN Page - Configure users, set up email notifications, manage display groups, access documentation, and link a Barracuda Backup Server.

Mobile Access

View the status of your Barracuda Backup Servers and devices connected through Barracuda Appliance Control. Additionally, you can contact Barracuda Networks Technical Support for assistance and, if necessary, open a support tunnel for your devices using Barracuda Networks Mobile Applications:

- Barracuda Networks iOS Mobile Application for iPhone and iPod Touch
- Barracuda Networks iOS Mobile Application for iPad

What's New in Barracuda Backup

What's New in Release 5.4

The following new major features have been added to Barracuda Backup version 5.4
Offsite Vaulting

- Store older backup data revisions offsite
- Specify monthly and yearly offsite retention policies

Granular SharePoint Restores

- Use Kroll Ontrack to restore SharePoint objects

Kroll Ontrack

You must have an active Kroll Ontrack license.

Continuing support for Microsoft applications:

- Microsoft SQL Server 2012
- Microsoft Exchange 2013
- Microsoft Windows 8 / 2012 (including ReFS)
- Microsoft Hyper-V 2012 Standalone
- Microsoft Hyper-V 2012 Clustering
- Microsoft Hyper-V 2008R2 Clustering

Introduction of the Barracuda Backup Agent (Linux):

- Adds ACL protection
- Adds alternate stream protection
- Adds extended attributes protection

Parallel VMware Backups:

- Multiple guests on the same host will be backed up concurrently

Improved Restore Browser:

- Adds ability to search for items
- Adds ability to select multiple items for restore

Advanced Graphs

What's New in Release 5.2

The following new major features have been added to Barracuda Backup version 5.2

- Barracuda LiveBoot in the Cloud for VMware:
  - Instantly boot to your VMware virtual machine using Barracuda Networks' deduplicated cloud storage.
  - Centralized management of LiveBoot instances

The following feature has been deprecated in version 5.2:

Watched Files:

- The seldomly used Watched Files feature has been deprecated in firmware versions 5.2, and will not be supported for new Barracuda Backup Servers. Note that existing Watched File Rules will continue to function as expected.

What's New in Release 5.1

The following new major features have been added to Barracuda Backup version 5.1

- copy.com Integration:
  - Share and back up folders and files backed up in the cloud via Copy.
- Backup Analytics:
  - View a detailed list of large items by source or file name in the **REPORTS > Large Items** page.

What's New in Release 5.0

The following new major features have been added to Barracuda Backup version 5.0

- Barracuda LiveBoot for VMware:
  - Instantly boot to your VMware environment any backed up snapshot using de-duplicated storage on Barracuda Backup Server
- Barracuda LiveBrowse for VMware:
  - View and traverse file structure inside all backed up VMware snapshots
  - Download Files and Directories within VMware snapshots
- Improved Restore Browser:
  - Cloud UI Restore Browser displays in the Barracuda Backup web interface
  - Download file system directories as ZIP files
  - Download email mailboxes and folders as ZIP files
- Reporting:

- Cloud UI Reports available in the Barracuda Backup web interface
- Size, Duration, Speed, and Type details are included in Reports
- Enhanced Backup and Restore reporting data organization

Deployment Options

In this Section

- Barracuda Backup Deployment Template
- Site-to-Site Deployment
- Site-to-Cloud Deployment
- Barracuda Cloud Storage Deployment Overview

Related Articles

- Barracuda Backup Replacement and Data Migration
- Backing Up Data Sources

Barracuda Backup Deployment Template

This article refers to Barracuda Backup firmware version 5.1 and higher.

In this article:

- Before Getting Started
- Physically Install and Configure the Barracuda Backup Server
- Firewall Ports
- Create a Barracuda Cloud Control Account
- Standard Activation
- Reseller (MSP) Activation
- Authentication and System Configuration Notes
- Create Backup Schedules
- Modify Your Backup Rate Limit
- Exclude Files from a Backup
- Create Data Retention Policies
- Replicate Data to another Barracuda Backup
- View Reports
- Create Display Groups

Related Articles

- Barracuda Backup Server Panel Indicators, Ports, and Connectors
- Barracuda Backup Server Hardware Specifications

Configuration Guidelines
This article is intended as a configuration *guideline;* your deployment will be specific to your environment. Any administrative changes should be reviewed with your IT team before proceeding.

This template is a based on a *typical onsite deployment* of the Barracuda Backup Server, and describes the initial setup.

Before Getting Started

You may need configuration access to the servers you intend to add as Backup source devices. If deemed necessary, you may also need permissions to make firewall changes. To facilitate your deployment, collect the information about your data sources and environment as shown in **Table 1.**

Table 1. Data Source Details.

Click here to expand...

Systems	**Details**	
Server Operating Systems	• Total number of each type of system • Whether system is physical or virtual, and if virtual, are they clustered	
If you are running Microsoft Exchange	• Version of each database • Number of databases running each version	
If you are running Microsoft SQL	• Version of each database • Number of databases running each version	
If you are running any other messaging or database system	• Type of messaging or database system • Version of each database • Number of databases running each version	
Other environments	• RIS/PACS • Enterprise Vault • Check warehousing/storage (financial) • Imaging systems storage • Source code repositories • DFS servers (4+ TB)	
Data	**Details**	
Data Retention	• Expected retention period on backup data • List exceptions	
Message-level backups or email archiving	Determine if email retention period differs from standard backup retention schedule	
Raw data	Total approximate raw data expected to back up in TB	
Network Information	**Details**	
Data Replication (provide bandwidth details)	• Barracuda Cloud Control • Another Barracuda Backup device (Private Cloud)	
Connection	Wan or low bandwidth	
Firewall or QoS device	Note any servers separated from the Barracuda Backup Server through a Firewall or QoS device (either network device or local host based system)	
Internal network	10.128.0.0/9 subnet	
Internal connection	Do internal connections from the Barracuda Backup Server to the network use 1GB copper, 10GB copper, or 10GB fiber?	
Alternative Backup Software/Conflicts	**Details**	

Other Backup Systems	- Note any servers with a backup agent or other backup product - Note whether another backup solution will be running in parallel with the Barracuda Backup Server	

Physically Install and Configure the Barracuda Backup Server

ⓘ The following instructions apply to Barracuda Backup Server models 390 and above; model 190 is a desktop unit.

Physically install the Barracuda Backup Server using the following steps:

1. Fasten the Barracuda Backup Server to a 19-inch rack or place it in a stable location.
2. Connect an Ethernet cable from the network switch to the Ethernet port on the back of the Barracuda Backup Server.

   ⓘ **Models 891, 991, 1091**
   The Barracuda Backup Server models 891, 991, and 1091 use multimode fiber optics via an LC connection with auto negotiation.

3. Connect a standard VGA monitor, PS2/USB keyboard, and an AC power cord to the Barracuda Backup Server.
4. Press the **Power** button on the front panel to turn the unit on.

By default, your Barracuda Backup Server is configured to obtain an IP address on your network using DHCP; if DHCP is acceptable, proceed to the section **Firewall Ports**, however, if you need to specify a static IP address, connect a monitor and keyboard to the Barracuda Backup Server using the instructions in the article How to Edit Network Settings through the Barracuda Console.

Table 2. AC Input Voltage Range.
Click here to expand...

Model	Power	AC Input Range	BTU/hr
190	Single 60W	12V	205
390	Single 220W	100V	751
490	Single 350W	100-240V	1194
690	Single 350W	100-240V	1194
890/891/892	720W Redundant Power	100-240V	2457
990/991	800W Redundant Power	100-240V	2730
1090/1091	1400W Redundant Power	100-140V 180-240V 120-230V	4777

Firewall Ports

If the Barracuda Backup Server is located behind a corporate firewall, open the following ports on the firewall to ensure proper communication between the Barracuda Backup Server and Barracuda Networks: 80, 443, 1194, and 5120-5129 outbound for both TCP and UDP traffic; Barracuda uses ports 5120-5129 for replicating data to a different location such as the cloud. The Barracuda Backup Server uses these ports to transfer data over the Internet to the offsite storage location. If you would like to restrict outbound network traffic on these ports to only reach Barracuda Networks, contact Barracuda Networks Technical Support.

Create a Barracuda Cloud Control Account

You must have a Barracuda Cloud Control account to use Barracuda Backup. If you do not already have an account, follow these steps:

1. Go to the following URL: http://login.barracudanetworks.com/
2. Complete the fields on the **Create New Account** page, and click **Submit**.

Standard Activation

Use the following steps to link your Barracuda Backup Server:

Click here to expand...

1. Go to http://login.barracudanetworks.com/, and log in.
2. Once logged in, click **Backup Service** in the left pane. If this is your first time linking a Barracuda Backup Server, click **Start Backup Service Setup**; otherwise, click **Link a Barracuda Backup Server** in the left pane.
3. On the **Validation** page, enter the serial number and the linking code for your Barracuda Backup Server from the sticker located on your Quick Start Guide that shipped with the device, and click **Continue**.
4. Complete the form and choose a Cloud Storage subscription plan if you intend to replicate data to Barracuda Cloud Storage; no Cloud Storage subscription is required for site-to-site replication.
5. In the web interface, if the Barracuda Backup Server is listed in the left pane with a green status light to the right of its name, proceed to the next section, otherwise, contact Barracuda Networks Technical Support.

Reseller (MSP) Activation

Use the following steps to link customer Barracuda Backup Servers:

Click here to expand...

1. Go to http://login.barracudanetworks.com/, and log in using a registered reseller account.
2. Once logged in, click **Backup Service** in the left pane, and click **Link a Barracuda Backup Server** in the left pane.
3. On the **Validation** page, enter the serial number and the linking code for the customer Barracuda Backup Server, and select the option that states 'I am a reseller and this Barracuda Backup Server is for my customer', entering the domain and username for the end-user account.
4. The end-user is sent an email verifying the serial number is to be added to their account.
5. Once verified, both the end-user and reseller can access the Barracuda Backup Server.
6. If the Barracuda Backup Server is listed in the left pane with a green status light to the right of its name, proceed to the next section, otherwise, contact Barracuda Networks Technical Support .

Update Server Settings and Firmware

From the **SYSTEM > BBS Settings** page, you can add and update Barracuda Backup Server settings including:

Click here to expand...

1. **Backup Server Name** - Name used to identify the currently selected Barracuda Backup Server in the web interface
2. **Backup Server Time Zone** - The time zone where the currently selected Barracuda Backup Server is located
3. **Backup Server Location** - The physical location of the Barracuda Backup Server including city, state, and country
4. **Backup Server Display Group** - The display group in which the Barracuda Backup Server resides
5. **Manage your display groups** - Click to add or remove a display group in the **ADMIN > Display Groups** page

When you log into Barracuda Backup, if there is a newer version of firmware available, the **STATUS** page displays a notification banner across the top of the page. To update the firmware, g o to the **SYSTEM > Firmware** page, and click **Upgrade Now** to immediately begin the firmware upgrade, or click **Dismiss** to hide the banner until the next time you log into the web interface.

From the **SYSTEM > Firmware** page, you can select the firmware upgrade policy:

Click here to expand...

1. **Current Installed Version** - Displays the currently installed firmware version
2. **Firmware Upgrade Policy** - Select the release stage you wish to update to the latest firmware
3. **Firmware Available** - Specifies the latest firmware version available based on the selected **Upgrade Policy**
4. **Upgrade Now** - If a newer version of firmware is available, click **Upgrade Now** to upgrade the firmware
5. **View release notes** - Click to view the Barracuda Backup release notes

> **Additional Information**
> For additional information, refer to the BBS Settings Page.

Configure Backup Source Devices

Use the following steps to set up systems located on the same network as your Barracuda Backup Server as backup source devices.

> **Additional Information**
> - For additional details on configuring backups and a list of supported data types, refer to the article How to Configure Backups.
> - For more information on setting up specific Backup Source Devices, for example, Microsoft Exchange Server 2007, refer to the

section Backing Up Data Sources.

1. Log into the web interface, go to **BACKUPS > Sources**, and click **Add Computer**.
2. Enter the backup source details:
    - Enter an identifying label for the source device in the **Computer Description** field.
    - In the **Computer Name** field, enter the FQDN or IP address of the source device; values *must* be resolvable on your local network.
    - Select the device **Computer Type**.
    - If appropriate for your data source, turn on **Enable File Share Backups**.
3. Click **Save**; the **Add Data Source** page displays.
4. Select the appropriate **Data Type**.
5. To replicate to Barracuda Cloud Storage, turn on **Replicate to Barracuda Cloud Storage**; if you have globally selected to replicate all data to Barracuda Cloud Storage for this Backup Server, this option is automatically turned **On**.
6. Continue with the configuration information and save the changes.

    > ⓘ For Windows-based agent shares, if you want to be able to do a bare metal recovery, make sure to back up all system volumes and system state.

    > ⓘ **Connection Information**
    >
    > - Requested connection details are based on the selected **Server Type**.
    > - The Barracuda Backup Agent (Windows) is enabled by default for Windows Servers; install the Agent from the **SYSTEM > Software Downloads** page in the web interface.
    > - To back up network file shares, turn on **Enable File Share Backups**, and enter your credentials.

Authentication and System Configuration Notes

Click here to expand...

- *Backups for Mac OS X/Linux/UNIX (SSH Connections)*
  Barracuda Backup uses an SSH (Secure Shell) client to access data contained on Mac OS X or Linux / Unix based computers running an SSH daemon. The SSH client uses public key cryptography to establish a secure connection to the SSH daemon.
  You must configure SSH access to any Mac OS X or Linux / UNIX computer you want to back up. Follow the on-screen instructions on the **BACKUP > Sources > Add Computer** page according to the operating system.
- *Directory-Based File Shares*
  When you back up a file share you must specify the share name on the network before you can select the folders to be backed up. On a Windows machine, a share name can be a drive volume such as "C$", or a folder and its associated subfolders such as "My Documents". At a minimum you will need *Read* access to the data that you are backing up and *Change Access* or *Full Control* to the shares in order to perform a restore. For Mac OS X and Linux / Unix-based computers with SSH connections, the share name should be the entire path to the directory you would like to back up, e.g., /home/<user>.
  When you select folders for backup you should begin by selecting the folders at the top of the folder tree hierarchy, and then deselect folders lower in the hierarchy that you do not want to back up. You can also specify an optional exclusion rule, which is applied when the backup runs to rule out files that do not meet your back up criteria.
- *Message-Level Backup: Microsoft® Exchange and Novell® GroupWise™*
  When you select the Message-Level Backup data type, you must supply the authentication information to access your mail server before you can select which mailboxes to back up. In addition to the authentication information provided on the Barracuda Backup web interface, you must configure the Message-Level settings on your Exchange or GroupWise server.
  For Microsoft Exchange servers, refer to Exchange Message-Level Backups for detailed instructions for configuring message-level backups.
  For GroupWise 8 and above, refer to GroupWise Message-Level Backups for detailed instructions for configuring message-level backups.

> ⓘ **Supported Data Types**

For additional information, refer to the Supported Data Types section.

Create Backup Schedules

Note that schedules are automatically created (with the default set to back up every day at 8:00PM) when a data source is created *except* if a schedule specifying *all* data sources already exists.

Now that you have configured your computers and data sources, you can create backup schedules, either individually or for all sources. If no schedule is created for a data source then it will not be backed up.

To create a backup schedule:

Click here to expand...

Go to the **BACKUP > Schedules** page of the Barracuda Backup web interface. Click **Add a Schedule** and fill in the information on the **Add Backup Schedule** page:

- **Schedule Name** - Enter a label to identify the backup schedule.
- **Items to Back Up** - Turn **Apply to All Computers and Data Sources for this Barracuda Backup Server** on to back up all content, or turn off, then expand and select the items you want to back up.
- **Schedule Timeline** - Turn on the days you want the back up to run.
- **Daily Backup Timeline** - Enter the start time; turn on **Repeat** if you want to specify a time period and end date to repeat the backup.

If the backup schedule is for Microsoft SQL or Microsoft Exchange, you must specify the type of backup to run:

- **Full** - This backup type performs a full backup of data, including the transaction logs.
- **Log** - This backup type only backs up transaction logs created since the last full backup.
- **Smart** - This backup type is a combination of the full backup and the transaction log backup, minimizing the impact of backups on network resources necessary to transfer data offsite. Barracuda Networks recommends this backup type for SQL and Exchange servers.

With the Smart Backup type, threshold values are used to determine when to switch between full and log backups. The minimum threshold value specifies how many days Barracuda Backup continues to back up transaction logs before another full backup is run. After the minimum threshold value is met, Barracuda Backup determines whether to perform another backup based on the binary data queue. If the binary data queue size exceeds 1 GB, Barracuda Backup continues the transaction log backup until:

- the maximum threshold level is met, or
- the queue size drops below 1 GB

Modify Your Backup Rate Limit

This step is optional. Rate limits control the data replication rate to Barracuda Cloud Storage or other offsite storage locations. You can limit Internet bandwidth consumption during peak usage times, and schedule backups for non-peak hours.

Your initial offsite backup may take on the order of days to complete but all of the data is backed up locally on the Barracuda Backup Server during this period. After the initial large transfer is complete, replicating your data offsite should complete with only a few hours of transfer each day. By default, Barracuda Backup is configured to run full speed data transfers at night so that bandwidth is not affected while most people are at work. An alternate rate limit allows you to adjust the limit speed and time interval.

The length of transfer time it will take to get your data offsite is impacted by the compression and deduplication rates on your data, the uplink speed of your Internet connection, the amount of data that changes every day, and any speed limits you apply to Barracuda Backup.

To adjust the backup rate limit:

Click here to expand...

1. On the **BACKUP > Rate Limit** page, select a Barracuda Backup Server on the left menu and create or edit the rate limit.
2. You can specify a default rate limit and an alternate rate limit which is maintained only during the specified time periods.

Exclude Files from a Backup

This step is optional. You can create exclusion rules that use pattern matching to identify directory or file names that are not to be backed up. Files which are typically excluded from backups include temporary files, music, movies and other files which are not essential for business needs.

Use the following steps to create an exclusion rule:

Click here to expand...

1. Go to the **BACKUP > Exclusions** page of the Barracuda Backup web interface. Click **Add an Exclusion**.
2. Fill in the information on the **Add an Exclusion** page:
    - **Exclusion Rule Name** - Enter a descriptive label to identify the exclusion rule.
    - **Add Exclusions to Reports** - Turn on to include exclusions in reports, and turn off if you do not want to include exclusions in the reports.
    - **Apply Recursively to Sub Directories -** Specify whether to apply the exclusion rule recursively to sub directories.
    - **Where to Exclude** - Turn **Apply to All Computers and Data Sources for this Barracuda Backup Server** on to apply the exclusion rule to all computers and data sources for the selected Barracuda Backup Server, or turn off, then expand and select the items to which to apply the exclusion rule.
3. In the **What to Exclude** section, specify what to exclude:
    - From the **Preset Expressions** menu, select the content you want to exclude, for example, **Video files**, then click **Add**.
    - In the **Expressions** field, enter a search string to exclude, for example, ***.mp3**, then click **Add**.
4. Click **Save** at the top of the page to add the exclusion rule.

To edit an existing exclusion rule, go to the **BACKUP > Exclusions** page of the Barracuda Backup web interface, and click **Edit** following the exclusion rule you want to edit. Make the necessary changes, then click **Save**.

To delete an exclusion rule, go to the **BACKUP > Exclusions** page of the Barracuda Backup web interface, and click the **Delete** icon following the exclusion rule you want to remove. Click **OK** to remove the rule.

Create Data Retention Policies

Data is retained based on a traditional grandfather-father-son (daily-weekly-monthly) rotation model. You can specify how long to keep daily, weekly, monthly, and yearly backups by creating data retention policies. Different retention policies can be created for different sets of data including files, data backed up by the Barracuda Backup Agent (Exchange, SQL, System State), and email messages.

You can create one policy for all of the computers and data sources on a Barracuda Backup Server or multiple policies that each include some subset of the data.

To set retention policies:

Click here to expand...

1. Go to the **BACKUP > Retention Policies** page, click **Add a Retention Policy**, and enter a name to identify the policy.
2. In the **Items to Retain** section, specify the data sources to which the retention policy applies; the **Retention Timeline** section displays. Select a timeline template on which to base your retention policy, or specify your own revision timeline.
3. Select the desired **Removed Files Rule** setting, and click **Save**.

When data is removed according to a retention policy, it is deleted from both the local Barracuda Backup Server and the offsite storage locations. Removed files that have been backed up using Network File Shares Protocol or SSHFS may be retained for a longer period of time, according to the configuration. Otherwise, once your data has been purged, it is gone forever. Purging applies to historic file revisions only; your current data is not impacted by a retention policy.

Replicate Data to another Barracuda Backup

Before configuring a backup destination, verify the following:

1. Make sure that your retention policies are configured before configuring replication. Otherwise you may waste bandwidth copying data that does not need to be replicated.
2. Verify Internet connectivity between the local and remote Barracuda Backup Server(s). Configuring a secure VPN connection between multiple Barracuda Backup Servers ensures the highest level of security possible.
3. You must have the serial number and replication code of the *destination* Barracuda Backup Server. Go to the *destination* Barracuda Backup Server, and go to the **BACKUP > Replication** page. The serial number and replication code display at the top right of the page.

⚠ **Important**

- Only the Barracuda Backup Server 490 and higher can act as a backup to other Barracuda Backup Servers, although any Barracuda Backup Server can *send* data.
- Data can be backed up to both a second Barracuda Backup Server and to Barracuda Cloud Storage. Data that is backed up on a second Barracuda Backup Server *cannot* be backed up yet again onto another Barracuda Backup Server.
- For every Terabyte of data replicated, Barracuda Networks recommends a 1.5 Mbps or T1 connection.
- You must have the serial number and replication code of the destination. These can be found by selecting the destination Barracuda Backup Server and looking at its **BACKUP > Replication** page.

Barracuda Backup Servers that are used to back up the data from one or more Barracuda Backup Servers are known as destinations. Data from one Barracuda Backup Server can be replicated to one or more destinations.

To configure where data is replicated to from a Barracuda Backup Server,

1. Select the Barracuda Backup Server in the list to which you wish to *add* a replication destination, and go to the **BACKUP > Replication** page.
2. To add a replication destination, click **Add a Target**.
3. In the **Add Destination** page, select from one of the following options:
    - From the **Backup Server** list, select a Barracuda Backup Server from your account to automatically load the required destination details, *or*
    - Enter the following details in the associated fields:
        - Enter the destination hostname or IP address
        - Enter the Serial Number from the *destination* Barracuda Backup Server
        - Enter the Replication Code from the *destination* Barracuda Backup Server
4. Click **Save**.

Once a destination is added, it appears in the **Sending Data To** table. If the status displays as online (Online ●), the two systems are able to communicate with each other.

On the **BACKUP > Replication** page, there is a global flag to replicate all data to either Barracuda Cloud Storage or to Barracuda Backup Servers:

☑ Send All Local Backups ●

If you wish to send data from diverse sources to both of these options, then *do not* set this flag on any items in the Target List. Instead, edit each data source on the **BACKUP > Sources** page, and specify where its data is to be replicated.

Edit Replication Server Settings

To edit the replication target settings, click **Settings** in the **Target List**. In the **Replication Target Settings** list, you can modify the destination IP address, disable data replication, and specify whether to send all data on the Barracuda Backup Server to this target.

Remove a Barracuda Backup Server

To permanently remove a replication destination, click **Remove** in the **Target List**.

Send Data To/Receiving Data From

Destination Barracuda Backup Servers display in the **Sending Data To** table. If a Barracuda Backup Server is acting as a destination for another Barracuda Backup Server, it displays in the **Receiving Data From** table.

View Reports

Barracuda Backup provides detailed reports including:

Click here to expand...

- **Backup Reports** - From the **REPORTS > Backup** page, you can view detailed reports for each backup that is run including any back up process that is currently running. Backup reports include details about the backup such as when the backup started, duration, size, if there were any errors or warnings, and any new, changed, or removed items. Reports also include links to each backed up file to view or download the item from the report.

  Click **Details** to view recent activity in chart form. You can also view a list of backed up files including the number of new, changed, and removed files, as well as a list of any errors encountered during backup.

  If a backup is currently in progress, the **REPORTS > Backup** page displays this information and allows you to cancel the backup.

  Click **View Past Reports** to access archived backup reports in the **Backup (Archived)** page. You can specify the number of reports you wish to display on the page, or enter a date range and click **Update** to display the archived reports.
- **Restore Report** - View restoration details in the **REPORTS > Restore** page.

  Click **Details** to view all details for the selected restoration including any encountered errors. Expand the detail tabs to view specific file errors and a list of restored files.
- **Large Items Report** - View a detailed list of large items by source or file name in the **REPORTS > Large Items** page. From the **Sources** drop-down menu, you can select to view large items by individual sources or for **All** sources. To further refine the report, enter a string in the **Filename contains** field, and click **Filter**. The report displays only those large items matching the filename content for the selected **Source**.

Create Display Groups

If you have multiple Barracuda Backup Servers, you can manage them through display groups. Go to the **ADMIN > Display Groups** page, and follow the on-screen instructions.

Additional Information
For additional information, refer to Display Groups Page.

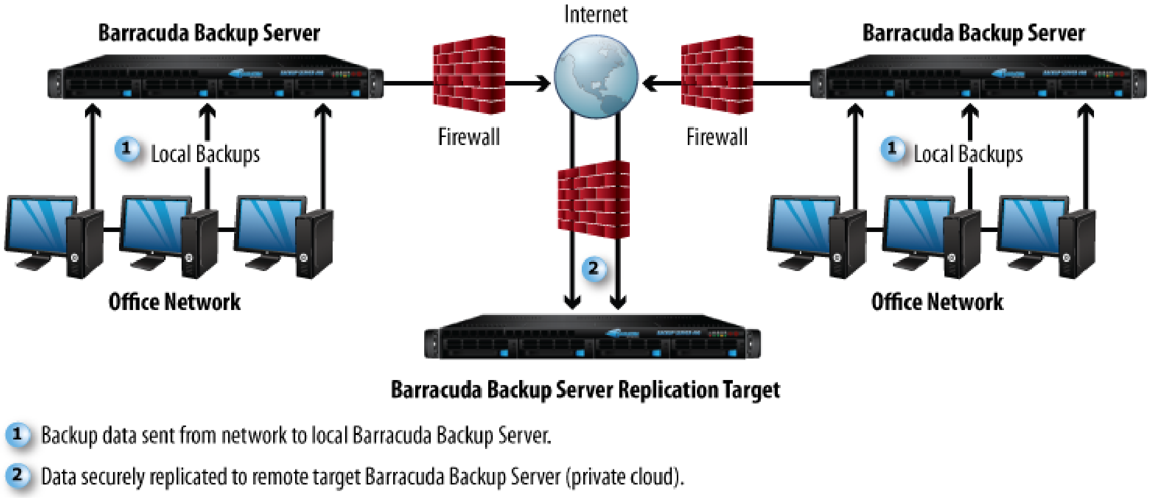
Site-to-Site Deployment

This article assumes each Barracuda Backup Server in the deployment is physically installed and connected to the network.

In this article:

- Configure the Barracuda Backup Server
  - Create a Barracuda Cloud Control Account
  - Configure the IP Address and Network Settings
  - Configure Your Corporate Firewall
  - Link Your Barracuda Backup Server to an Account
  - Add the Server Name and Location
  - Create Display Groups
- Configure Data Sources
  - Add Systems and Select Data Sources
  - Create Backup Schedules
  - Create Data Retention Policies
  - Modify Your Back Up Rate Limit
- Secure the Barracuda Backup Server
  - Communication and Configuration
  - Data Transmission and Storage
  - Management Access
  - Encryption
- Configure Replication
- Restore Data from Replication Destinations

In a site-to-site deployment, a Barracuda Backup Server acts as a backup or "private cloud" to replicate data from one or more Barracuda Backup Servers. Each Barracuda Backup Server can send data to one or more other Barracuda Backup Servers. In the following image, a target Barracuda Backup Server acts as a backup to two other Barracuda Backup Servers:


Barracuda Backup Server
Internet
Barracuda Backup Server
Firewall
Firewall
1 Local Backups
1 Local Backups
Office Network
Office Network
2
Barracuda Backup Server Replication Target
1 Backup data sent from network to local Barracuda Backup Server.
2 Data securely replicated to remote target Barracuda Backup Server (private cloud).

Configure the Barracuda Backup Server

Use the following steps to configure your Barracuda Backup Server.

Create a Barracuda Cloud Control Account

You must have a Barracuda Cloud Control account to use Barracuda Backup. If you do not already have an account, follow these steps:

1. Go to the following URL: http://login.barracudanetworks.com/
2. Complete the fields on the **Create New Account** page, and click **Submit**.

Configure the IP Address and Network Settings

By default, the Barracuda Backup Server is configured to obtain an IP address on your network using DHCP. If you want to assign it a static IP address instead, you can configure it using the console administration interface. If not, skip the following steps:

To configure the Barracuda Backup Server to use a static IP address:

1. Connect a monitor and keyboard to the Barracuda Backup Server.
2. Use your arrow keys to highlight the **DHCP/Static** field.
3. Using the spacebar select **Static** for your IP address assignment preference.
4. Enter the IP Address, Netmask, Default Gateway, Primary DNS Server, and Secondary DNS Server (optional) as appropriate for your network.
5. Click **Enter** on the **Commit Changes** box.

Once changes are committed, the Barracuda Backup server attempts to connect to Barracuda Networks.

The LAN and Internet boxes on the console administration interface are green when the Barracuda Backup Server is determined to be online. The Barracuda box remains red until it is linked to an account later in the installation process.

Configure Your Corporate Firewall

If the Barracuda Backup Server is located behind a corporate firewall, you may need to open the following ports to allow communication between the Barracuda Backup Server and the Internet. In site-to-site deployment, you can specify the ports to use for replication on the **BACKUP > Replication** page, or optionally, you can replicate over ports 5120-5129.

- Ports 1194 and 5120-5129 outbound for both TCP and UDP traffic. The ports are used to transfer data to either Barracuda Cloud Storage or to another Barracuda Backup Server over the Internet.

> **Cloud Replication**
> If you would like to restrict the outbound network traffic on these ports to Barracuda Cloud Storage, contact Barracuda Networks Technical Support for a list of the IP addresses to allow.

Link Your Barracuda Backup Server to an Account

Your Barracuda Backup Server must be linked to your Barracuda Cloud Control Account before you can initiate data backups.

To link your Barracuda Backup Server:

1. Go to this URL: http://login.barracudanetworks.com/
2. Sign in with your **Username** and **Password**.
3. If Barracuda Backup is your default or only Barracuda Networks product, then the Barracuda Backup web interface appears. If not, click **Backup Service** at the top of the screen.
4. Click **Start Backup Service Setup**, and then select the **STATUS** tab.
5. Click **Link a Barracuda Backup Server**.
6. Enter your **Serial Number** and **Linking Code** from the sticker attached to the Quick Start Guide that shipped with your Barracuda Backup Server. These values are case sensitive. The Serial Number can also be found on a sticker on the back of the unit. Follow the on-screen prompts to complete linking and to supply your account information.
7. The linking process may take a few minutes to complete. Wait until the **STATUS** page appears, indicating that the Barracuda Backup Server is successfully linked to your account. A green light next to the Barracuda Backup Server on the **STATUS** page indicates that your Barracuda Backup Server has successfully connected.

Add the Server Name and Location

Use the **SYSTEM > BBS Settings** page to view or modify the Barracuda Backup Server details including server name, time zone, physical location, and display group:

- **Backup Server Name** - Name used to identify the currently selected Barracuda Backup Server in the web interface

- **Backup Server Time Zone** - The time zone where the currently selected Barracuda Backup Server is located
- **Backup Server Location** - The physical location of the Barracuda Backup Server including city, state, and country
- **Backup Server Display Group** - The display group in which the Barracuda Backup Server resides
- **Manage your display groups** - Click to add or remove a display group in the **ADMIN > Display Groups** page

Create Display Groups

This step is optional. If you have multiple Barracuda Backup Servers, you can manage them by creating display groups on the **ADMIN > Display Groups** page.

> **Additional Information**
> See the Display Groups Page for more information.

Configure Data Sources

This section describes how to configure backups.

Add Systems and Select Data Sources

There may be more than one data source on each server, and each can have unique back up characteristics.

> **Additional Information**
> - See Backup Up Data Sources for details by data source type.
> - See Data Backup Tasks for step-by-step instructions on setting up data sources.

Create Backup Schedules

> Note that schedules are automatically created (with the default set to back up every day at 8:00PM) when a data source is created *except* if a schedule specifying *all* data sources already exists.

Now that you have configured your computers and data sources, you can create backup schedules, either individually or for all sources. If no schedule is created for a data source then it will not be backed up.

> **Additional Information**
> See the Schedules Page for more information.

Create Data Retention Policies

Data is retained based on a traditional grandfather-father-son (daily-weekly-monthly) rotation model. You can specify how long to keep daily, weekly, monthly, and yearly backups by creating data retention policies. Different retention policies can be created for different sets of data including files, data backed up by a Barracuda Backup Agent, and email messages.

You can create one policy for all of the computers and data sources on a Barracuda Backup Server or multiple policies that each include some subset of the data.

> **Additional Information**
> - See the Retention Policies Page for more information.
> - See Creating Effective Retention Policies for revision timelines, removed file rules, and removed email timelines.

Modify Your Back Up Rate Limit

This step is optional. Rate limits control the data replication rate to Barracuda Cloud Storage or other offsite storage locations. You can limit Internet bandwidth consumption during peak usage times, and schedule backups for non-peak hours.

> **Additional Information**
> See the Rate Limit Page for more information.

Exclude Files from a Backup

This step is optional. You can create exclusion rules that use pattern matching to identify directory or file names that are not to be backed up. Files which are typically excluded from backups include temporary files, music, movies and other files which are not essential for business needs in the **BACKUP > Exclusions** page.

Additional Information
See the Exclusions Page for more information.

Check Backup Reports

View reports on an ongoing basis as needed. The **REPORTS > Backup** page contains detailed backup reports. A list of in progress backups displays at the top of the page, and once a backup is complete, a detailed report displays in a table by device. Click **Details** following the report you want to view.

Additional Information
See the Reports Page for more information.

Secure the Barracuda Backup Server

This section describes how to secure your Barracuda Backup Servers.

Communication and Configuration

Administration and backup configuration that is set using the Barracuda Backup web interface is sent to the Barracuda Backup Server via a 256-bit encrypted VPN tunnel. The Barracuda Backup Server uses HTTPS port 1194 to send status updates to Barracuda Backup. Data transfers are initiated by the Barracuda Backup Server rather than by Barracuda Cloud Storage or a remote Barracuda Backup Server.

Data Transmission and Storage

Data transferred between your network and Barracuda Cloud Storage, or between your network and a remote Barracuda Backup Server, is always encrypted. File parts are AES 256-bit symmetrically encrypted before they are stored, and they remain encrypted until a restore is requested.

Management Access

- **Monitor Activity** - You can check the user activity page periodically for authentication attempts, changes to settings, and updates to account information. Go to the **ADMIN > User Activity Reports** page to see all activity for an account, including logins and when a user has enabled or disabled replication.
- **Restrict Logins by IP Address** - You can restrict access to Barracuda Backup to one or more IP addresses. On the **ADMIN > Users** page, click the **Edit** graphic (✏) to edit a user account; enter an IP address or a range.
- **Secure Network Access** - HTTPS is always used for secure web browser communication with Barracuda Backup.

Encryption

Data transfers from the local Barracuda Backup Server to a receiving Barracuda Backup Server are always encrypted. Data is stored compressed and encrypted at rest on the receiving Barracuda Backup Server; the local Barracuda Backup Server does not store in an encrypted or compressed state. The most aggressive combination of symmetrical and asymmetrical encryption in the industry keeps your data stored in a format that nobody but you can access. The United States government recently approved 192-bit AES encryption as the preferred method for protecting top-secret information. The Barracuda Backup solution starts with even higher 256-bit AES encryption.

In addition, Barracuda Networks has developed a proprietary advanced digital cataloging system that breaks down your data into small pieces and tracks the changes of these parts over time, and strips the original meta identifiers from your files.

As data is transmitted to the remote Barracuda Backup Server, your symmetrically-encrypted data parts are compressed and sent over your Internet connection with an asymmetrically-encrypted key.

Configure Replication

This section describes how to configure replication.

Important

- Only the Barracuda Backup Server 490 and higher can act as a backup to other Barracuda Backup Servers, although any Barracuda Backup Server can *send* data.
- Data can be backed up to both a second Barracuda Backup Server and to Barracuda Cloud Storage. Data that is backed up on a second Barracuda Backup Server *cannot* be backed up yet again onto another Barracuda Backup Server.
- For every Terabyte of data replicated, Barracuda Networks recommends a 1.5 Mbps or T1 connection.
- You must have the serial number and replication code of the destination. These can be found by selecting the destination Barracuda Backup Server and looking at its **BACKUP > Replication** page.

Barracuda Backup Servers that are used to back up the data from one or more Barracuda Backup Servers are known as destinations. Data from one Barracuda Backup Server can be replicated to one or more destinations.

To configure where data is replicated to from a Barracuda Backup Server,

1. Select the Barracuda Backup Server in the list to which you wish to *add* a replication destination, and go to the **BACKUP > Replication** page.
2. To add a replication destination, click **Add a Target**.
3. In the **Add Destination** page, select from one of the following options:
   - From the **Backup Server** list, select a Barracuda Backup Server from your account to automatically load the required destination details, *or*
   - Enter the following details in the associated fields:
     - Enter the destination hostname or IP address
     - Enter the Serial Number from the *destination* Barracuda Backup Server
     - Enter the Replication Code from the *destination* Barracuda Backup Server
4. Click **Save**.

Once a destination is added, it appears in the **Sending Data To** table. If the status displays as online (Online ●), the two systems are able to communicate with each other.

On the **BACKUP > Replication** page, there is a global flag to replicate all data to either Barracuda Cloud Storage or to Barracuda Backup Servers:

☑ Send All Local Backups ●

If you wish to send data from diverse sources to both of these options, then *do not* set this flag on any items in the Target List. Instead, edit each data source on the **BACKUP > Sources** page, and specify where its data is to be replicated.

Edit Replication Server Settings

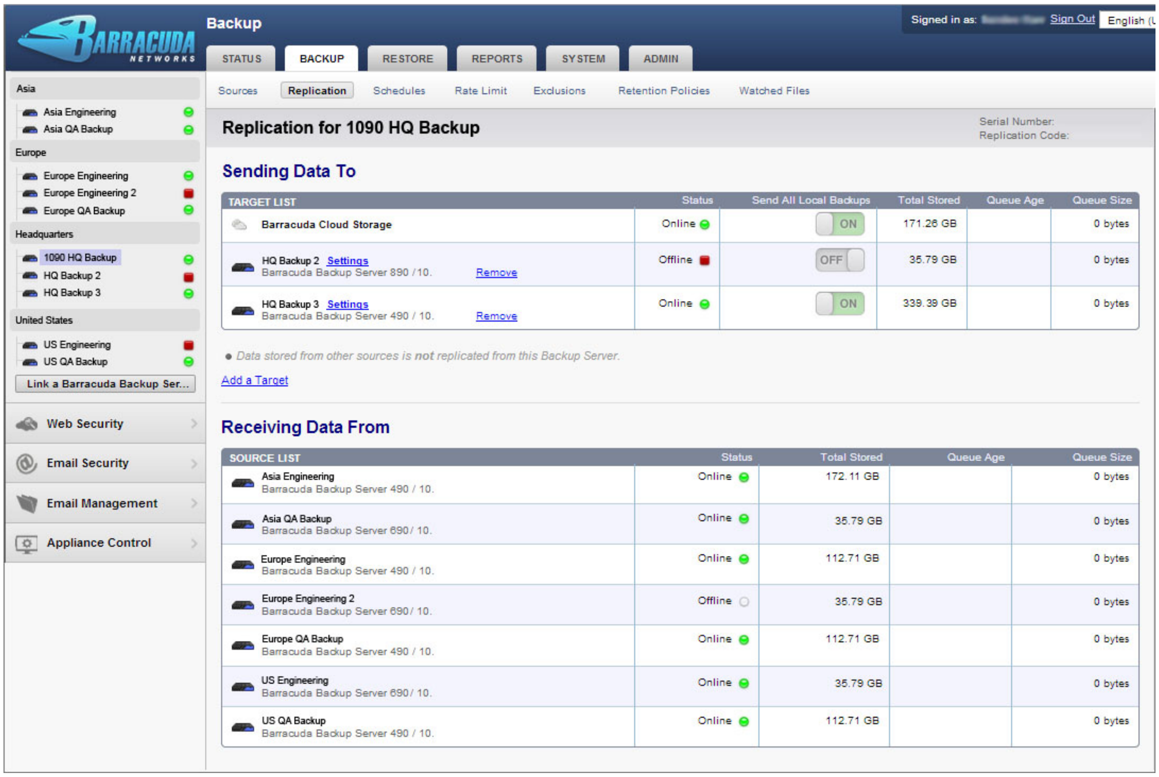
To edit the replication target settings, click **Settings** in the **Target List**. In the **Replication Target Settings** list, you can modify the destination IP address, disable data replication, and specify whether to send all data on the Barracuda Backup Server to this target.

Remove a Barracuda Backup Server

To permanently remove a replication destination, click **Remove** in the **Target List**.

Send Data To/Receiving Data From

Destination Barracuda Backup Servers display in the **Sending Data To** table. If a Barracuda Backup Server is acting as a destination for another Barracuda Backup Server, it displays in the **Receiving Data From** table.


Backup
Signed in as: [redacted] Sign Out
English (U
STATUS
BACKUP
RESTORE
REPORTS
SYSTEM
ADMIN
Sources
Replication
Schedules
Rate Limit
Exclusions
Retention Policies
Watched Files
Asia
Asia Engineering
Asia QA Backup
Europe
Europe Engineering
Europe Engineering 2
Europe QA Backup
Headquarters
1090 HQ Backup
HQ Backup 2
HQ Backup 3
United States
US Engineering
US QA Backup
Link a Barracuda Backup Ser...
Web Security
Email Security
Email Management
Appliance Control

Replication for 1090 HQ Backup

Serial Number:
Replication Code:

Sending Data To

TARGET LIST	Status	Send All Local Backups	Total Stored	Queue Age	Queue Size
Barracuda Cloud Storage	Online ●	ON	171.26 GB		0 bytes
HQ Backup 2 Settings Barracuda Backup Server 890 / 10. Remove	Offline 🟥	OFF	35.79 GB		0 bytes
HQ Backup 3 Settings Barracuda Backup Server 490 / 10. Remove	Online ●	ON	339.39 GB		0 bytes

- *Data stored from other sources is **not** replicated from this Backup Server.*

Add a Target

Receiving Data From

SOURCE LIST	Status	Total Stored	Queue Age	Queue Size
Asia Engineering Barracuda Backup Server 490 / 10.	Online ●	172.11 GB		0 bytes
Asia QA Backup Barracuda Backup Server 690/ 10.	Online ●	35.79 GB		0 bytes
Europe Engineering Barracuda Backup Server 490 / 10.	Online ●	112.71 GB		0 bytes
Europe Engineering 2 Barracuda Backup Server 690/ 10.	Offline ○	35.79 GB		0 bytes
Europe QA Backup Barracuda Backup Server 490 / 10.	Online ●	112.71 GB		0 bytes
US Engineering Barracuda Backup Server 690/ 10.	Online ●	35.79 GB		0 bytes
US QA Backup Barracuda Backup Server 490 / 10.	Online ●	112.71 GB		0 bytes

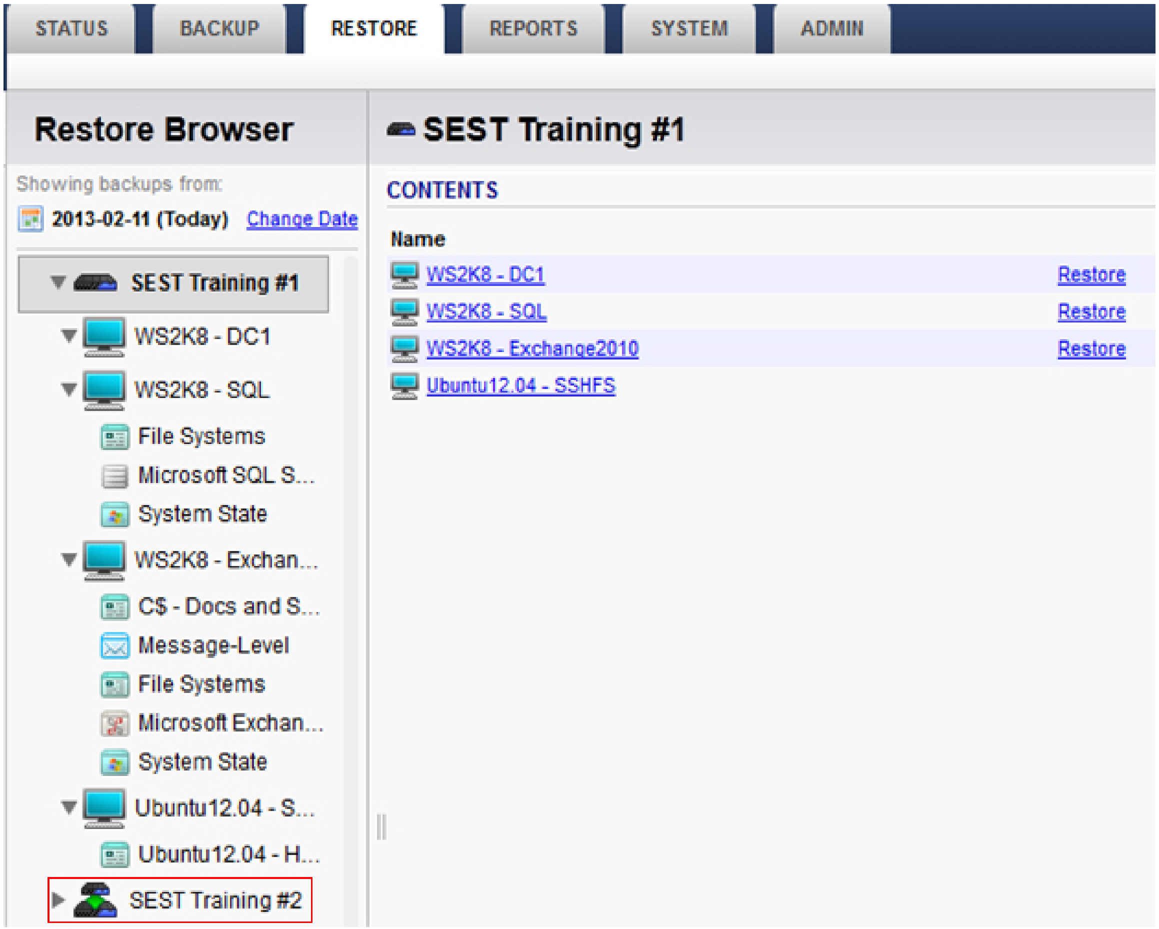
Additional Information
See the Replication Page for more information.

Restore Data from Replication Destinations

Only the Barracuda Backup Server 490 and higher can act as a backup to other Barracuda Backup Servers, although any Barracuda Backup Server can *send* data.

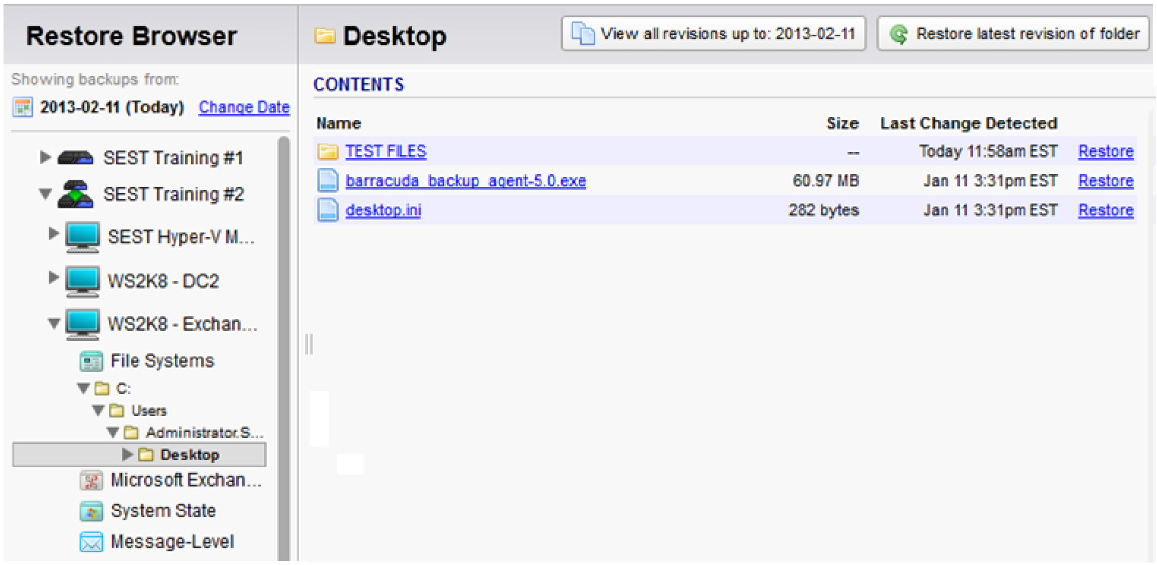
To restore from a replication destination,

1. Log into the Barracuda Backup web interface, and select the *receiving* Barracuda Backup Server from which to restore.
2. Go to the **Restore> Restore Browser** page, and in the left pane select the *sending* Barracuda Backup Server that you are receiving data from:


STATUS
BACKUP
RESTORE
REPORTS
SYSTEM
ADMIN
Restore Browser
Showing backups from:
2013-02-11 (Today)
Change Date
SEST Training #1
WS2K8 - DC1
WS2K8 - SQL
File Systems
Microsoft SQL S...
System State
WS2K8 - Exchan...
C$ - Docs and S...
Message-Level
File Systems
Microsoft Exchan...
System State
Ubuntu12.04 - S...
Ubuntu12.04 - H...
SEST Training #2
SEST Training #1
CONTENTS

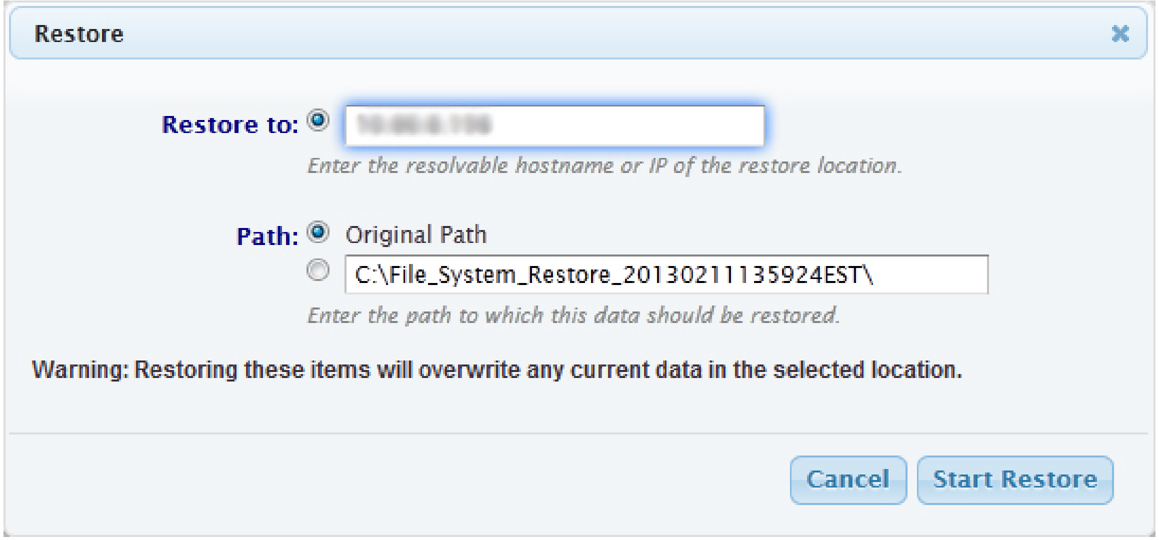
Name	
WS2K8 - DC1	Restore
WS2K8 - SQL	Restore
WS2K8 - Exchange2010	Restore
Ubuntu12.04 - SSHFS	

3. Expand the *sending* Barracuda Backup Server to review its backup sources, and click on the server or computer from which to restore; the contents displays in the right pane:


Restore Browser
Showing backups from:
2013-02-11 (Today)
Change Date
SEST Training #1
SEST Training #2
SEST Hyper-V M...
WS2K8 - DC2
WS2K8 - Exchan...
File Systems
C:
Users
Administrator.S...
Desktop
Microsoft Exchan...
System State
Message-Level
Desktop
View all revisions up to: 2013-02-11
Restore latest revision of folder
CONTENTS

Name	Size	Last Change Detected	
TEST FILES	--	Today 11:58am EST	Restore
barracuda_backup_agent-5.0.exe	60.97 MB	Jan 11 3:31pm EST	Restore
desktop.ini	282 bytes	Jan 11 3:31pm EST	Restore

4. In the **Contents** section, click **Restore** next to the file or directory for restore. The Restore window displays.
5. In the **Restore to** field, enter the hostname or IP address of the *restore to* location. In the **Path** section, select the **Original Path**, or you can designate a new location:



Restore to: ● [redacted]
Enter the resolvable hostname or IP of the restore location.

Path: ● Original Path
○ C:\File_System_Restore_20130211135924EST\
Enter the path to which this data should be restored.

Warning: Restoring these items will overwrite any current data in the selected location.

6. Click **Start Restore**. Once the restore is complete, go to **REPORTS > Restore** to verify the restore completed successfully.

Configuring Replication

> Any Barracuda Backup Server can *send* data to another Barracuda Backup Server, however, only Barracuda Backup Servers 490 and higher can act as a backup to other Barracuda Backup Servers.
>
> For every Terabyte of data replicated, Barracuda Networks recommends a 1.5 Mbps or T1 connection.

In this article:

- Before Starting Replication
- Verify Retention Policies
- Configure Destinations
- Specify Data Replication Destination
- Temporarily Disable a Destination
- Remove a Destination
- Loss of Communication

Related Articles

- Replication
- Site-to-Site Deployment
- Setting Up Site-to-Site Replication

Before Starting Replication

Verify Internet connectivity between the local and remote Barracuda Backup Server(s). Configuring a secure VPN connection between multiple Barracuda Backup Servers ensures the highest level of security possible.

Verify Retention Policies

Make sure that your retention policies are configured before configuring replication. Otherwise you may waste bandwidth copying data that does not need to be replicated. On the Barracuda Backup Server, go to the **BACKUP > Retention Policies** page and verify that the retention policies are configured before configuring replication to avoid copying data that does not need replication.

Verify Internet connectivity between the local and remote Barracuda Backup Server(s). Configuring a secure VPN connection between multiple Barracuda Backup Servers ensures the highest level of security.

Configure Destinations

Barracuda Backup Servers that are used to back up the data from one or more Barracuda Backup Servers are known as *destinations*. Data from one Barracuda Backup Server can be replicated to one or more destinations.

Note: Before you can configure a destination, you must have the target Barracuda Backup Server serial number and replication code. To locate these values, select the target Barracuda Backup Server in the list, and go to the **BACKUP** > **Replication** page. The serial number and replication code display to the right of the target Barracuda Backup Server name.

1. Select the Barracuda Backup Server in the list, and go to the **BACKUP > Replication** page.
2. Click the **Add a Target link**.
3. Enter the target Barracuda Backup Server IP address or hostname, serial number, and replication code. Click **Save**.
4. The server displays in the **Sending Data To** table.

When the status displays as **Online** the two systems are able to communicate with each other.

Specify Data Replication Destination

1. Select the Barracuda Backup Server in the list, and go to the **BACKUP > Replication** page.
2. In the **Sending Data To** table, in the **Global Setting** column, you specify whether to replicate all data to Barracuda Cloud Storage or to a Barracuda Backup Servers. To send data from diverse sources to both of these options, do not turn on the flag. Instead, edit each data source on the **BACKUP > Sources** page, and specify where its data is replicated.

Temporarily Disable a Destination

You can temporarily disable site-to-site replication for one or more destinations. If it is disabled, nothing is sent from the Barracuda Backup Server to the destination until the feature is enabled or until 24 hours have passed. This allows you to move the destination system to a remote location, say, without getting backup errors. If the 24 hours pass and site-to-site replication is not manually re-enabled, the Barracuda Backup Servers attempt to communicate with each other and, if successful, perform the backups.

1. Select the Barracuda Backup Server in the list, and go to the the **BACKUP > Replication** page.
2. In the **Sending Data To** table, click on the **Settings** link beside the destination Barracuda Backup Server.
3. On the **Replication Target Settings** page, turn off **Enable Data Replication**.

Remove a Destination

1. Select the Barracuda Backup Server in the list, and go to the the **BACKUP > Replication** page.
2. In the **Sending Data To** table, click on the **Remove** link beside the destination Barracuda Backup Server.

Loss of Communication

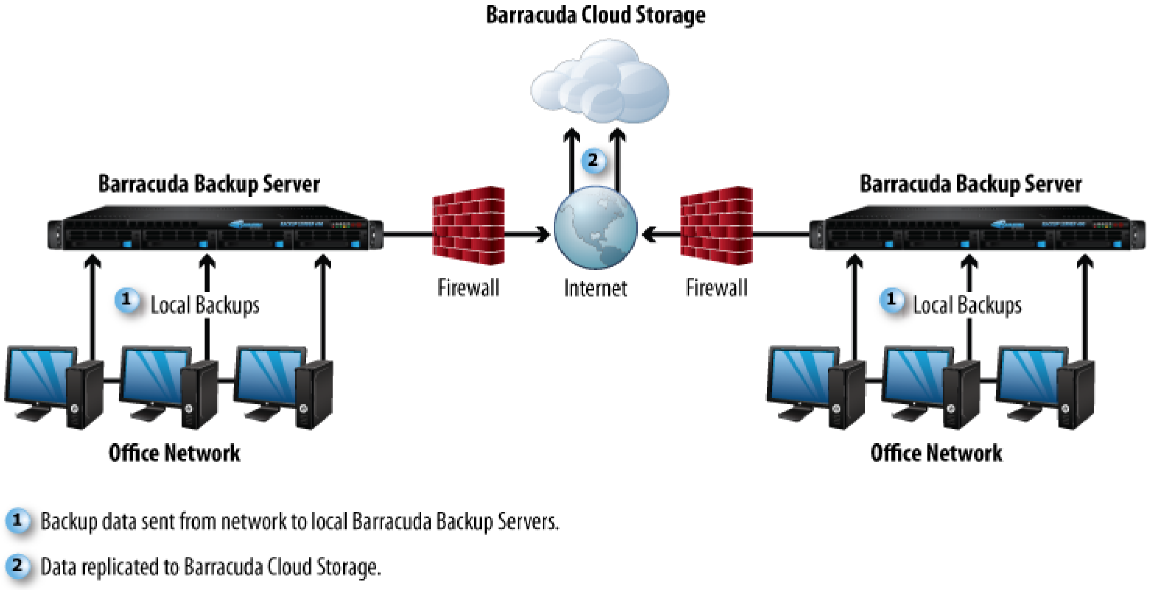
If there is a loss of communication between the Barracuda Backup Server and its back up destinations, the data to be be backed up is queued and errors are generated. Data is queued until the issue is resolved. The queue size in the table on the **BACKUP > Replication** page indicates how much data is waiting to be replicated. Not all of this data is actually copied to the destination; some of it is deduplicated as the replication proceeds. Only those parts that are not already stored in the remote location are sent over the Internet.

Site-to-Cloud Deployment

In this article:

- Configure the Barracuda Backup Server
- Configure Data Sources
- Secure the Barracuda Backup Server
- Configure Replication

Barracuda Cloud Storage subscription plans provide diverse offsite storage that scales to meet your changing data requirements. Barracuda Cloud Storage includes secure backup to two separate data centers. Storage is allocated in 200 gigabyte increments and is all disk-based. The following image shows two Barracuda Backup Servers replicating data to Barracuda Cloud Storage:


Barracuda Cloud Storage
2
Barracuda Backup Server
Barracuda Backup Server
Firewall
Internet
Firewall
1 Local Backups
1 Local Backups
Office Network
Office Network
1 Backup data sent from network to local Barracuda Backup Servers.
2 Data replicated to Barracuda Cloud Storage.

Configure the Barracuda Backup Server

Use the following steps to configure your Barracuda Backup Server.

Create a Barracuda Cloud Control Account

You must have a Barracuda Cloud Control account to use Barracuda Backup. If you do not already have an account, follow these steps:

1. Go to the following URL: http://login.barracudanetworks.com/
2. Complete the fields on the **Create New Account** page, and click **Submit**.

Configure the IP Address and Network Settings

By default, the Barracuda Backup Server is configured to obtain an IP address on your network using DHCP. If you want to assign it a static IP address instead, you can configure it using the console administration interface. If not, skip the following steps:

To configure the Barracuda Backup Server to use a static IP address:

1. Connect a monitor and keyboard to the Barracuda Backup Server.
2. Use your arrow keys to highlight the **DHCP/Static** field.
3. Using the spacebar select **Static** for your IP address assignment preference.
4. Enter the IP Address, Netmask, Default Gateway, Primary DNS Server, and Secondary DNS Server (optional) as appropriate for your network.
5. Click **Enter** on the **Commit Changes** box.

Once changes are committed, the Barracuda Backup server attempts to connect to Barracuda Networks.

The LAN and Internet boxes on the console administration interface are green when the Barracuda Backup Server is determined to be online. The Barracuda box remains red until it is linked to an account later in the installation process.

Configure Your Corporate Firewall

If the Barracuda Backup Server is located behind a corporate firewall, you may need to open the following ports to allow communication between the Barracuda Backup Server and the Internet.

- Ports 1194 and 5120-5129 outbound for both TCP and UDP traffic. The ports are used to transfer data to either Barracuda Cloud Storage or to another Barracuda Backup Server over the Internet. In site-to-site deployment, data can be replicated either over ports 5120-5129 or over a set of ports you specify on the **BACKUP > Replication** page.

  Cloud Replication
  If you would like to restrict the outbound network traffic on these ports to Barracuda Cloud Storage, contact Barracuda Networks Technical Support for a list of the IP addresses to allow.

Link Your Barracuda Backup Server to an Account

Your Barracuda Backup Server must be linked to your Barracuda Cloud Control Account before you can initiate data backups.

To link your Barracuda Backup Server:

1. Go to this URL: http://login.barracudanetworks.com/
2. Sign in with your **Username** and **Password**.
3. If Barracuda Backup is your default or only Barracuda Networks product, then the Barracuda Backup web interface appears. If not, click **Backup Service** at the top of the screen.
4. Click **Start Backup Service Setup**, and then select the **STATUS** tab.
5. Click **Link a Barracuda Backup Server**.
6. Enter your **Serial Number** and **Linking Code** from the sticker attached to the Quick Start Guide that shipped with your Barracuda Backup Server. These values are case sensitive. The Serial Number can also be found on a sticker on the back of the unit. Follow the on-screen prompts to complete linking and to supply your account information.
7. The linking process may take a few minutes to complete. Wait until the **STATUS** page appears, indicating that the Barracuda Backup Server is successfully linked to your account. A green light next to the Barracuda Backup Server on the **STATUS** page indicates that your Barracuda Backup Server has successfully connected.

Add the Server Name and Location

Use the **SYSTEM > BBS Settings** page to view or modify the Barracuda Backup Server details including server name, time zone, physical location, and display group:

- **Backup Server Name** - Name used to identify the currently selected Barracuda Backup Server in the web interface
- **Backup Server Time Zone** - The time zone where the currently selected Barracuda Backup Server is located
- **Backup Server Location** - The physical location of the Barracuda Backup Server including city, state, and country
- **Backup Server Display Group** - The display group in which the Barracuda Backup Server resides
- **Manage your display groups** - Click to add or remove a display group in the **ADMIN > Display Groups** page

Define Display Groups

This step is optional. If you have multiple Barracuda Backup Servers, you can manage them by creating display groups on the **ADMIN > Display Groups** page.

> **Additional Information**
> See the Display Groups Page for more information.

Configure Data Sources

This section describes how to configure backups.

Add Systems and Select Data Sources

Set up your data sources on the **BACKUP > Sources** page, and specify that you want to **Replicate to Barracuda Cloud Storage** on the **Add Data Source** page. You may have more than one data source on each server, and each can have unique back up characteristics. For set up details by data source type, see Backup Up Data Sources.

> **Additional Information**
> See Data Backup Tasks for more information.

Create Backup Schedules

> Note that schedules are automatically created (with the default set to back up every day at 8:00PM) when a data source is created *except* if a schedule specifying *all* data sources already exists.

Now that you have configured your computers and data sources, you can create backup schedules, either individually or for all sources. If no schedule is created for a data source then it will not be backed up.

Additional Information
See the Schedules Page for more information.

Create Data Retention Policies

Data is retained based on a traditional grandfather-father-son (daily-weekly-monthly) rotation model. You can specify how long to keep daily, weekly, monthly, and yearly backups by creating data retention policies. Different retention policies can be created for different sets of data including files, data backed up by a Barracuda Backup Agent, and email messages.

You can create one policy for all of the computers and data sources on a Barracuda Backup Server or multiple policies that each include some subset of the data.

Additional Information

- See the Retention Policies Page for more information.
- See Creating Effective Retention Policies for revision timelines, removed file rules, and removed email timelines.

Modify Your Backup Rate Limit

This step is optional. Rate limits control the data replication rate to Barracuda Cloud Storage or other offsite storage locations. You can limit Internet bandwidth consumption during peak usage times, and schedule backups for non-peak hours.

Additional Information
See the Rate Limit Page for more information.

Exclude Files from a Backup

This step is optional. You can create exclusion rules that use pattern matching to identify directory or file names that are not to be backed up. Files which are typically excluded from backups include temporary files, music, movies and other files which are not essential for business needs in the **BACKUP > Exclusions** page.

Additional Information
See the Exclusions Page for more information.

Check Backup Reports

View reports on an ongoing basis as needed. The **REPORTS > Backup** page contains detailed backup reports. A list of in progress backups displays at the top of the page, and once a backup is complete, a detailed report displays in a table by device. Click **Details** following the report you want to view.

Additional Information
See the Reports Page for more information.

Secure the Barracuda Backup Server

This section describes how to secure your Barracuda Backup Servers.

Communication and Configuration

Administration and backup configuration that is set using the Barracuda Backup web interface is sent to the Barracuda Backup Server via a 256-bit encrypted VPN tunnel. The Barracuda Backup Server uses HTTPS port 1194 to send status updates to Barracuda Backup. Data transfers are initiated by the Barracuda Backup Server rather than by Barracuda Cloud Storage.

Data Transmission and Storage

Data transferred between your network and Barracuda Cloud Storage is always encrypted. File parts are AES 256-bit symmetrically encrypted before they are stored, and they remain encrypted until a restore is requested.

Management Access

- **Monitor Activity** - You can check the user activity page periodically for authentication attempts, changes to settings, and updates to account information. Go to the **ADMIN > User Activity Reports** page to see all activity for an account, including logins and when a user has enabled or disabled replication.
- **Restrict Logins by IP Address** - You can restrict access to Barracuda Backup to one or more IP addresses. On the **ADMIN > Users** page, click the **Edit** graphic (✏) to edit a user account; enter an IP address or a range.
- **Secure Network Access** - HTTPS is always used for secure web browser communication with Barracuda Backup.

Encryption

Data transfers between the local Barracuda Backup Server and a remote Barracuda Backup Server are always encrypted. Data is stored compressed and encrypted at rest. The most aggressive combination of symmetrical and asymmetrical encryption in the industry keeps your data stored in a format that nobody but you can access. The United States government recently approved 192-bit AES encryption as the preferred method for protecting top-secret information. The Barracuda Backup solution starts with even higher 256-bit AES encryption.

In addition, Barracuda Networks has developed a proprietary advanced digital cataloging system that breaks down your data into small pieces and tracks the changes of these parts over time, and strips the original meta identifiers from your files.

As data is transmitted to the remote Barracuda Backup Server, your symmetrically-encrypted data parts are compressed and sent over your Internet connection with an asymmetrically-encrypted key.

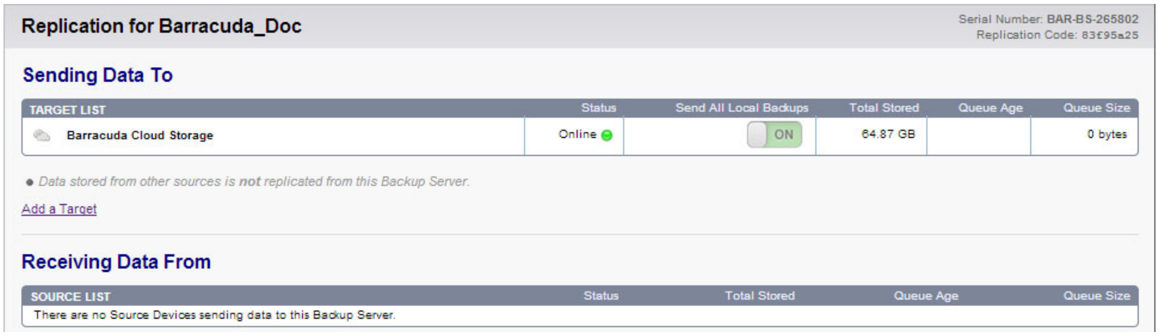
Configure Replication

This section describes how to configure replication to Barracuda Cloud Storage.

Globally Replicate Data

You can select to globally replicate all data from all data sources for the currently selected Barracuda Backup Server to Barracuda Cloud Storage on the **Replication** page:

1. Select the Barracuda Backup Server in the left pane, and then go to the **BACKUP > Replication** page.
2. In the **Sending Data To** section, turn *On* **Send All Local Backups**:



Replication for Barracuda_Doc

Serial Number: BAR-BS-265802
Replication Code: 83f95a25

Sending Data To

TARGET LIST	Status	Send All Local Backups	Total Stored	Queue Age	Queue Size
Barracuda Cloud Storage	Online ●	ON	64.87 GB		0 bytes

● *Data stored from other sources is **not** replicated from this Backup Server.*

Add a Target

Receiving Data From

SOURCE LIST	Status	Total Stored	Queue Age	Queue Size
There are no Source Devices sending data to this Backup Server.				

Selectively Replicate Data

You can specify which data sources are replicated to the cloud for the currently selected Barracuda Backup Server:

1. Select the Barracuda Backup Server in the left pane, and then go to the **BACKUP > Replication** page.
2. In the **Sending Data To** section, set **Send All Local Backups** to **Off**.
3. Go to the **BACKUP > Sources** page, and click **Edit** next to the data sources listed in the right section of the page.
4. On the **Edit** page, turn on **Replicate to Barracuda Cloud Storage**, and then click **Save**.

> **Data Sources**
> You can specify **Replicate to Barracuda Cloud Storage** when setting up your data sources as described in the section Add Systems and Select Data Sources.

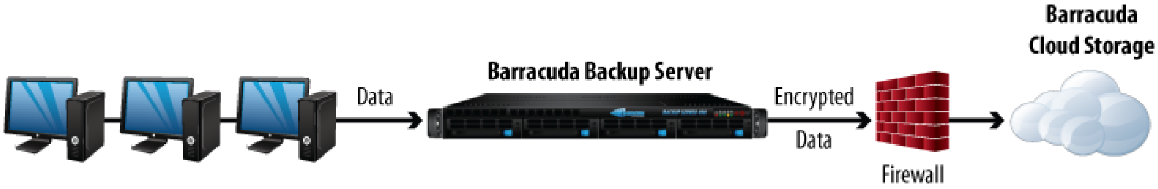
Additional Information

- See the Replication Page for more information.

Barracuda Cloud Storage Deployment Overview

You can deploy a Barracuda Backup Server with backups stored on Barracuda Cloud Storage.

In the following image, a Barracuda Backup Server is located in a network and its backups are stored on Barracuda Cloud Storage:



Storage Plans

Barracuda Cloud Storage is available through either a subscription plan or by purchasing Unlimited Cloud Storage. In firmware release 5.4 and higher, you can enable offsite vaulting which leverages Barracuda's Cloud Storage service to offload up to twelve monthly and seven yearly revisions to strictly cloud storage, freeing up disk space on your local Barracuda Backup Server.

- **Cloud Storage subscription** – Barracuda's Cloud Storage subscription plans provide diverse offsite storage options that scale to meet your changing data requirements. Storage plans are purchased in 200 GB increments and are all disk-based, allowing you to scale up or down depending on your organizations' needs.
- **Unlimited Cloud Storage** - Unlimited Cloud Storage allows you to store all of your content without having to manage storage usage limits.

Unlimited Cloud Storage mirrors content offsite based on your retention policies. As noted above, in firmware release 5.4 and higher, you can enable offsite vaulting to purge data from the local cache.

Contact your Barracuda Sales Representative for subscription plan and Unlimited Cloud Storage pricing.

Getting Started

Recommended Steps

- Step 1: How to Install the Barracuda Backup Server
- Step 2: How to Configure Barracuda Backup
- Step 3: How to Configure Backups
- Step 4: Data Backup Tasks

Alternatively, you can download the Barracuda Backup Service Quick Start Guide from the Barracuda Backup Overview page.

Step 1: How to Install the Barracuda Backup Server

> Before installation, determine the best type of deployment for your Barracuda Backup Server; refer to the Deployment section for a list of options.

In this article:

- Create a Barracuda Cloud Control Account
- Verify the Equipment
- Connect to Network

Related Articles
• Replacement and Data Migration • How to Configure Barracuda Backup

Create a Barracuda Cloud Control Account

You must have a Barracuda Cloud Control account to use Barracuda Backup. If you do not already have an account, follow these steps:

1. Go to the following URL: http://login.barracudanetworks.com/
2. Complete the fields on the **Create New Account** page, and click **Submit**.

Verify the Equipment

Verify you have the necessary equipment:

- Barracuda Backup Server (check that you have received the correct model)
- AC power cord
- Ethernet cables
- VGA monitor (recommended)
- Keyboard (recommended)
- Barracuda Backup Server serial number and linking code (available on both the side of the Barracuda Backup Server and the Quick Start Guide card)
- Connectivity and access information for servers you want to back up
- All necessary cables, e.g., multi-mode fiber optic cable is necessary for models 891, 991, and 1091

Connect to Network

1. Fasten the Barracuda Backup Server to a standard 19-inch rack or other stable location.

   > ⚠ **Caution**
   > Do not block the cooling vents located on the front and rear of the unit.

2. Connect an Ethernet cable from your network switch to the Ethernet port on the back panel of the Barracuda Backup Server.
3. Connect the power cord, VGA monitor, and a keyboard to the Barracuda Backup Server. The AC input voltage range is 100-240 volts at 50/60 Hz.
4. Press the **POWER** button on the front panel to turn on the unit.

Continue with Step 2: How to Configure Barracuda Backup.

Step 2: How to Configure Barracuda Backup

> Before configuring the IP address and network settings, complete Step 1: How to Install a Barracuda Backup Server.

In this article:

- Configure the IP Address and Network Settings
- Configure Your Corporate Firewall
- Link Your Barracuda Backup Server to an Account
- Enter Server Name and Location
- Define Display Groups
- Add a Barracuda Backup Server to a Group

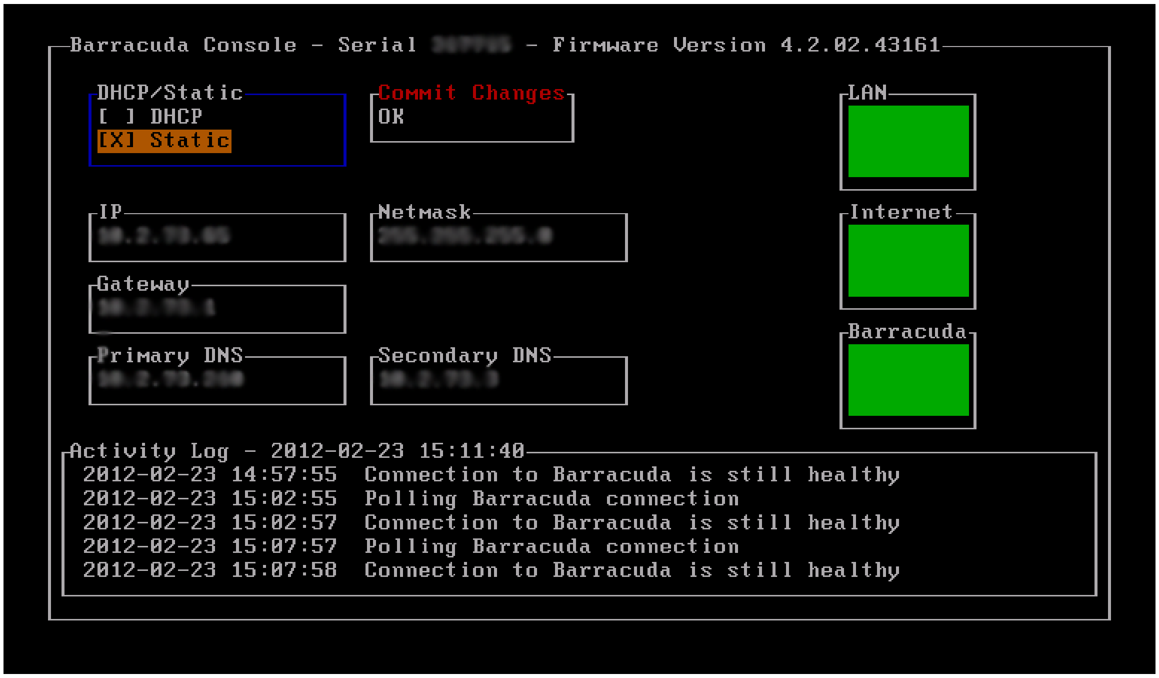
Related Articles
• Replacement and Data Migration • How to Link a Barracuda Backup Server • How to Unlink a Barracuda Backup Server • How to Edit Network Settings through the Barracuda Console • How to Configure Backups • Hardware Specifications • Panel Indicators, Ports, and Connectors

Configure the IP Address and Network Settings

By default, the Barracuda Backup Server is configured to obtain an IP address on your network using DHCP. If you want to assign it a static IP address instead, you can configure it using the console administration interface. If not, proceed to the section **Configure Your Corporate Firewall**:

To configure the Barracuda Backup Server to use a static IP address:

1. Connect a monitor and keyboard to the Barracuda Backup Server.
2. Use your arrow keys to highlight the **DHCP/Static** field.
3. Use the spacebar to select **Static** for your IP address assignment preference:



Barracuda Console - Serial [redacted] - Firmware Version 4.2.02.43161

DHCP/Static
[ ] DHCP
[X] Static

Commit Changes
OK

IP: [redacted]

Netmask: [redacted]

Gateway: [redacted]

Primary DNS: [redacted]

Secondary DNS: [redacted]

```
Activity Log - 2012-02-23 15:11:40
 2012-02-23 14:57:55  Connection to Barracuda is still healthy
 2012-02-23 15:02:55  Polling Barracuda connection
 2012-02-23 15:02:57  Connection to Barracuda is still healthy
 2012-02-23 15:07:57  Polling Barracuda connection
 2012-02-23 15:07:58  Connection to Barracuda is still healthy
```

4. Enter the IP Address, Netmask, Default Gateway, Primary DNS Server, and Secondary DNS Server (optional) as appropriate for your network.
5. Click **Enter** on the **Commit Changes** box.

Once changes are committed, the Barracuda Backup server attempts to connect to Barracuda Networks.

The LAN and Internet boxes on the console administration interface are green when the Barracuda Backup Server is determined to be online. The Barracuda box remains red until it is linked to an account later in the installation process.

For additional information, refer to the article How to Edit Network Settings through the Barracuda Console.

Configure Your Corporate Firewall

If the Barracuda Backup Server is located behind a corporate firewall, open the following ports on the firewall to ensure proper communication between the Barracuda Backup Server and Barracuda Networks: 80, 443, 1194, and 5120-5129 outbound for both TCP and UDP traffic; Barracuda uses ports 5120-5129 for replicating data to a different location such as the cloud. The Barracuda Backup Server uses these ports to transfer data over the Internet to the offsite storage location. If you would like to restrict outbound network traffic on these ports to only reach Barracuda Networks, contact Barracuda Networks Technical Support.

Link Your Barracuda Backup Server to an Account

Your Barracuda Backup Server must be linked to your Barracuda Cloud Control Account before you can initiate data backups.

To link your Barracuda Backup Server:

1. Go to this URL: **http://login.barracudanetworks.com/**
2. Sign in with your **Username** and **Password**.
3. If Barracuda Backup is your default or only Barracuda Networks product, then the Barracuda Backup web interface appears. If not, click **Backup Service** at the top of the screen.
4. Click **Start Backup Service Setup**, and then select the **STATUS** tab.

5. Click **Link a Barracuda Backup Server**.
6. Enter your **Serial Number** and **Linking Code** from the sticker attached to the Quick Start Guide that shipped with your Barracuda Backup Server. These values are case sensitive. The Serial Number can also be found on a sticker on the back of the unit. Follow the on-screen prompts to complete linking and to supply your account information.
7. The linking process may take a few minutes to complete. Wait until the **STATUS** page appears, indicating that the Barracuda Backup Server is successfully linked to your account. A green light next to the Barracuda Backup Server on the **STATUS** page indicates that your Barracuda Backup Server has successfully connected.

> For additional information, refer to the following articles:
>
> - How to Link a Barracuda Backup Server as a User or Reseller
> - How to Unlink a Barracuda Backup Server

Enter Server Name and Location

In the **SYSTEM > Barracuda Backup Server Settings** page, enter a name for your Barracuda Backup Server, the associated time zone, and server location.

Define Display Groups

If you have multiple Barracuda Backup Servers, you can manage them through display groups:

1. Log into Barracuda Backup, and go to the **ADMIN > Display Groups** page.
2. All display groups active on your account display in the **Current Display Groups** section.
3. To add a new display group, enter a name for the group of devices, and click **Add**. For example, if you want to group all Barracuda Backup Servers by location, you might create groups by geographic location: Engineering - Asia, Engineering - US, Engineering - Europe.
4. The display group name appears in the **Current Display Groups** section.
5. IfTo remove a display group, click **Remove** following the name of the group you want to remove; click **OK** to remove the group.

> If you delete a display group that contains devices, those devices are moved to the default group.

Add a Barracuda Backup Server to a Group

Once you create display groups, you can add a Barracuda Backup Server to the group using the following steps:

1. In the left pane, select the desired Barracuda Backup, and go to the **SYSTEM > BBS Settings** page.
2. In the **Backup Server Display Group** section, choose from the **Current Display Group** drop-down list, select the desired display group name.
3. To add or remove display groups, click **Manage your display groups** to go to the **ADMIN > Display Groups** page.
4. Click **Save**.

Continue with Step 3: How to Configure Backups.

Step 3: How to Configure Backups

> Before configuring the web interface, complete Step 2: How to Configure Barracuda Backup.

You can configure where your data is backed up and in what manner. This article refers to data sources, which are subsets of data on each server that is to be backed up.

In this article:

- Where Data is Backed Up
- Supported Data Types
  - Microsoft Server Applications
  - Microsoft Exchange Storage Group Backup

- Microsoft Exchange Server Message-Level Backups
- Novell GroupWise Message-Level Backup
- Microsoft SQL Server Backup
- Microsoft Hyper-V Virtual Machines
- Windows System State Backup
- VMware Host Storage
- Linux File Systems using the Barracuda Backup Agent (Linux)
- Macintosh OS X, Linux/Unix, and Novelle NetWare
- Network Addressable Storage

Related Articles

- Backing Up Data Sources
- Replicating Data
- Deployment Options

Where Data is Backed Up

You configure how and when your data is to be backed up. All data is first backed up to a local Barracuda Backup Server. If you have more than one local Barracuda Backup Server, you must decide which one backs up which systems.

Data on the local Barracuda Backup Server can then be backed up, or replicated, to another Barracuda Backup Server in a remote location, to the Barracuda Cloud Storage, or to a combination of the two. See Site-to-Site Deployment or Site-to-Cloud Deployment for deployment options. The location of the replicated data is specified for each data source. You can also choose to not replicate the backed-up data at all.

Supported Data Types

> **Configuration Details**
> For system-specific configuration details, refer to Backing Up Data Sources.

Choose the method for backing up data based on the type of data. The Barracuda Backup Server supports the following data sources:

- Microsoft Exchange Server and Exchange Server DAG
- Microsoft Hyper-V
- Microsoft SQL Server
- VMware
- How to Back Up Microsoft Active Directory
- How to Back Up and Restore a Microsoft SharePoint SQL Database
- Understanding IBM Domino Server Backup
- How to Configure GroupWise Message-Level Backups
- How to Set Up a Root Account to Back Up Macintosh OS X
- How to Back Up Linux/UNIX Data Using SSHFS
- Understanding Changed Block Tracking on Virtual Machines
- How to Enable Changed Block Tracking through the Barracuda Backup Web Interface
- How to Back Up Network Addressable Storage - NAS
- How to Back Up FirstClass Mail
- How to Back Up NFS Mounts with the Barracuda Backup Agent (Linux)
- How to Back Up NSS Mounts with the Barracuda Backup Agent (Linux)

Review the following sections for more information about specific data types.

Microsoft Server Applications

The Barracuda Backup Agent (Windows) provides application-aware backups for Microsoft® SQL Server, Microsoft Exchange Server (including message-level backup of mailboxes and messages), Microsoft System State, and Microsoft Hyper-V Server. The Agent also provides support for open file backups, and file attributes and permissions.

Install the Agent on every Microsoft Server that you want to back up; you can download and install the Barracuda Backup Agent (Windows) from the **SYSTEM > Software Downloads** page. Data sources that can be backed up using the Agent are automatically detected after the computer is identified on the **BACKUP > Sources** page

The Agent searches the NTFS change journal to track modified, added, or deleted files rather than searching the entire volume to improve Agent backup speed.

Microsoft Exchange Storage Group Backup

The Barracuda Backup Agent (Windows) provides a full backup of the Exchange storage group for Exchange Server 2003 and 2007. An Exchange storage group is a container for your email database and its associated system and transaction log files.

Microsoft Exchange uses transaction logging to commit new and changed data to the database, and to ensure that records of the transactions exist if a store is damaged between backups. The Exchange storage group, and its associated transaction logs, is the most important data to back up on your Exchange Server to ensure your email database is available in the event it becomes damaged or unrecoverable. If you must rebuild a server, you can use the latest transaction log files plus the last full backup to recover your database.

The Barracuda Backup Agent (Windows) backs up and restores the entire storage group; it allows for the storage group to be restored to a storage group or to an alternate Microsoft Exchange Server.

Microsoft Exchange Server Message-Level Backups

Message-level backup provides a quick way to restore single email messages to the original location or to an alternate mailbox. Message-level backup is not intended to be a disaster recovery option for your Microsoft Exchange environment. The Barracuda Backup Agent (Windows) allows you to back up the entire Exchange Information Store and should be used for disaster protection.

Novell GroupWise Message-Level Backup

Barracuda Backup connects directly to Novell® GroupWise to back up individual emails stored within user mailboxes.

Microsoft SQL Server Backup

The Barracuda Backup Agent (Windows) provides a complete backup of the Microsoft SQL Server including the master, user, model, msdb, and pubs databases.

Barracuda Networks recommends that all of the Microsoft SQL Server user databases be configured for full recovery model so that transaction logs can be backed up. This allows you to restore a user database to any point of time that is contained within a transaction log backup.

Some versions of the Microsoft SQL Server, such as SQL Express database, do not support full recovery model. If the full recovery model cannot be used, the Barracuda Backup Agent (Windows) performs full backups of the database each time a backup runs.

The Microsoft article Recovery Models (SQL Server), provides more information about the Microsoft SQL Server and its three database recovery models, and how to change the recovery model of a database.

> ⚠ **Important**
> Do not use other methods to back up Microsoft SQL Server databases, such as Microsoft or third-party utilities, when using the Barracuda Backup Agent (Windows). If you use more than one back up method on the same database, one or more of those methods causes the Microsoft SQL Server to truncate the transaction logs. This forces a full backup of the database every time, and can result in data that cannot be restored.

Barracuda Networks recommends that you back up the master database each time it is changed. The master database contains configuration information that is required to restore an instance of SQL Server.

Microsoft Hyper-V Virtual Machines

The Barracuda Backup Agent (Windows) provides application-aware backups for Microsoft Hyper-V hypervisor-based virtualization systems, and provides support for open file backups, file attributes, and permissions as well as automatic data source detection.

Windows System State Backup

The Barracuda Backup Agent (Windows) can back up and restore the Microsoft Windows System State. Microsoft Windows System State backups allow backup of critical system related components, including the local Registry, COM+ Class Registration Database, the System Boot Files, Active Directory Database Files (NTDS.DIT) for Domain Controllers, and the SYSVOL folder. A System State backup can be used to recover to a known good system state after a hardware or software crash.

System State data might not include all of the information required to recover a system from a failure. Barracuda Networks recommends that all boot and system volumes be backed up in addition to System State.

VMware Host Storage

Add VMware® host storage, including host configuration and virtual machine images, as data sources for backup and restoration through Barracuda Backup. You must be running a licensed copy of ESX, ESXi, or vCenter version 4.0 or later, and the VMware license must include access to the vSphere Data Recovery API. For details on CBT, refer to the article Understanding Changed Block Tracking on Virtual Machines.

Note that the entire VMware image is backed up each time back up is run.

Linux File Systems using the Barracuda Backup Agent (Linux)

Use the BarracudaBackup Agen (Linux) to back up Linux file systems such as Red Hat, Ubuntu, or SUSE. The Agent can back up open files, permissions, soft and hard links, and supports multiple data streams.

Macintosh OS X, Linux/Unix, and Novelle NetWare

Mac OS X, Linux/Unix, and Novell NetWare® systems are backed up using *File Share*. This method refers to the mechanism that uses standard network protocols, such as CIFS/Samba or SSHFS, to access your servers.

You can use the Barracuda Backup Agent (Linux) to back up Linux/UNIX-based file systems, such as Red Hat, Ubuntu, or SUSE. Use the Barracuda Backup Agent (Linux) to back up the selected items and protect any open files and permissions.

Network Addressable Storage

You can back up network addressable storage (NAS) data sources with CIFS and back up access control lists (ACL).

Continue with Step 4: Data Backup Tasks or go to Backing Up Data Sources.

Step 4: Data Backup Tasks

Before configuring the web interface, complete Step 3: How to Configure Backups.

Perform these tasks to configure your data for backup:

- Identify Systems to be Backed Up
- Select Type of Data to be Backed Up
- Create Backup Schedules
- Modify Your Backup Rate Limit
- Exclude Files from a Backup
- Create Data Retention Policies
- Check Backup Reports

Related Articles

- Sources Page
- Replication Page
- Schedules Page
- Rate Limit Page
- Exclusions Page
- Retention Policies Page
- Reports Page

Identify Systems to be Backed Up

For each local Barracuda Backup Server, identify the data sources that are to be backed up. There may be more than one data source on each server, and each can have unique backup characteristics.

1. Log in to Barracuda Backup, and select the associated Barracuda Backup Server in the left pane.
2. Go to the **BACKUP > Sources** page, and click **Add Computer** to identify the system; when you enter a set of user credentials on this page, the specified username is used for network file systems and **must have at least read access** to the data you intend to back up.

For Microsoft Windows and Novell Netware, you must enter both a username and password. For Mac OSX, Linux and UNIX (SSHFS), enter a username after you set up your SSH key.

> Alternately, you can download the Barracuda Backup Agent software from the **SYSTEM > Software Downloads** page (or in releases prior to 5.0, the **SUPPORT > Software Downloads** page), and install it on every computer to be backed up. For more information, refer to Barracuda Backup Agent (Windows) and Barracuda Backup Agent (Linux).
>
> Note that you must have 1 GB of free space to install the Barracuda Backup Agent software.

3. Once a computer is added, click **Save**. The **Add Data Source** page displays. Enter the data description and select the appropriate data type. For Windows-based agent shares, if you want to be able to do a bare metal recovery, make sure to back up all system volumes and system state.
4. Turn on **Replicate to Other Barracuda Backup Servers**, and click **Save**.
5. Complete steps 1 through 4 for each system and data source you want to back up.

> - ***If this is a Mac, UNIX, or Linux system***, follow the instructions on the **Add Computer** page to install a public key so that the Barracuda Backup Server is able to securely connect to it, then you can configure the data sources.
> - ***If this is a Novell Netware system***, enter the system information on the **Add Computer** page. When that is done, on the **Add Data Source** page you will be able to specify the data location. CIFS or SSHFS is used to back up the Netware data.
> - ***For all systems****,* when you enter a set of user credentials on this page, the specified username is used for network file systems and **must have at least read access** to the data you intend to back up. For Microsoft Windows and Novell Netware you must enter both a username and password. For Mac OSX, Linux and UNIX (SSHFS), you only need to enter a username after you set up your SSH key.
> - For Active Directory users, add the domain and then a **** in the username field. For example:
>   Username = **cuda\jsmith**

Select Type of Data to be Backed Up

After a computer has been added, select the data source(s) to be backed up on that computer:

1. From the **BACKUP > Sources** page, click **Add Data Source** next to the associated device from which you want to back up.
2. On the **Add Data Source** page, select the appropriate data type. For Windows-based agent shares, if you want to be able to do a bare metal recovery, make sure to back up all system volumes and system state.
3. To replicate to Barracuda Cloud Storage, turn on **Replicate to Barracuda Cloud Storage**; if you have globally selected to replicate all data to Barracuda Cloud Storage for this Backup Server, this option is automatically turned *On*.
4. Continue with the configuration information and save the changes.

Authentication and System Configuration Notes

Click here to expand...

- *Backups for Mac OS X/Linux/UNIX (SSH Connections)*
  Barracuda Backup uses an SSH (Secure Shell) client to access data contained on Mac OS X or Linux / Unix based computers running an SSH daemon. The SSH client uses public key cryptography to establish a secure connection to the SSH daemon.
  You must configure SSH access to any Mac OS X or Linux / UNIX computer you want to back up. Follow the on-screen instructions on the **BACKUP > Sources > Add Computer** page according to the operating system.
- *Directory-Based File Shares*
  When you back up a file share you must specify the share name on the network before you can select the folders to be backed up. On a Windows machine, a share name can be a drive volume such as "C$", or a folder and its associated subfolders such as "My Documents". At a minimum you will need *Read* access to the data that you are backing up and *Change Access* or *Full Control* to the shares in order to perform a restore. For Mac OS X and Linux / Unix-based computers with SSH connections, the share name should be the entire path to the directory you would like to back up, e.g., /home/<user>.
  When you select folders for backup you should begin by selecting the folders at the top of the folder tree hierarchy, and then deselect folders lower in the hierarchy that you do not want to back up. You can also specify an optional exclusion rule, which is applied when the backup runs to rule out files that do not meet your back up criteria.
- *Message-Level Backup: Microsoft® Exchange and Novell® GroupWise™*
  When you select the Message-Level Backup data type, you must supply the authentication information to access your mail server before you can select which mailboxes to back up. In addition to the authentication information provided on the Barracuda Backup web interface, you must configure the Message-Level settings on your Exchange or GroupWise server.
  For Microsoft Exchange servers, refer to Exchange Message-Level Backups for detailed instructions for configuring message-level backups.

For GroupWise 8 and above, refer to GroupWise Message-Level Backups for detailed instructions for configuring message-level backups.

Supported Data Types
For additional information, refer to the Supported Data Types section.

Create Backup Schedules

Note that schedules are automatically created (with the default set to back up every day at 8:00PM) when a data source is created *exce pt* if a schedule specifying *all* data sources already exists.

Now that you have configured your computers and data sources, you can create backup schedules, either individually or for all sources. If no schedule is created for a data source then it will not be backed up.

To create a backup schedule:
Click here to expand...

Go to the **BACKUP > Schedules** page of the Barracuda Backup web interface. Click **Add a Schedule** and fill in the information on the **Add Backup Schedule** page:

- **Schedule Name** - Enter a label to identify the backup schedule.
- **Items to Back Up -** Turn **Apply to All Computers and Data Sources for this Barracuda Backup Server** on to back up all content, or turn off, then expand and select the items you want to back up.
- **Schedule Timeline -** Turn on the days you want the back up to run.
- **Daily Backup Timeline** - Enter the start time; turn on **Repeat** if you want to specify a time period and end date to repeat the backup.

If the backup schedule is for Microsoft SQL or Microsoft Exchange, you must specify the type of backup to run:

- **Full** - This backup type performs a full backup of data, including the transaction logs.
- **Log** - This backup type only backs up transaction logs created since the last full backup.
- **Smart** - This backup type is a combination of the full backup and the transaction log backup, minimizing the impact of backups on network resources necessary to transfer data offsite. Barracuda Networks recommends this backup type for SQL and Exchange servers.

With the Smart Backup type, threshold values are used to determine when to switch between full and log backups. The minimum threshold value specifies how many days Barracuda Backup continues to back up transaction logs before another full backup is run. After the minimum threshold value is met, Barracuda Backup determines whether to perform another backup based on the binary data queue. If the binary data queue size exceeds 1 GB, Barracuda Backup continues the transaction log backup until:

- the maximum threshold level is met, or
- the queue size drops below 1 GB

Modify Your Backup Rate Limit

This step is optional. Rate limits control the data replication rate to Barracuda Cloud Storage or other offsite storage locations. You can limit Internet bandwidth consumption during peak usage times, and schedule backups for non-peak hours.

Your initial offsite backup may take on the order of days to complete but all of the data is backed up locally on the Barracuda Backup Server during this period. After the initial large transfer is complete, replicating your data offsite should complete with only a few hours of transfer each day. By default, Barracuda Backup is configured to run full speed data transfers at night so that bandwidth is not affected while most people are at work. An alternate rate limit allows you to adjust the limit speed and time interval.

The length of transfer time it will take to get your data offsite is impacted by the compression and de-duplication rates on your data, the uplink speed of your Internet connection, the amount of data that changes every day, and any speed limits you apply to Barracuda Backup.

To adjust the backup rate limit:
Click here to expand...

1. On the **BACKUP > Rate Limit** page, select a Barracuda Backup Server on the left menu and create or edit the rate limit.
2. You can specify a default rate limit and an alternate rate limit which is maintained only during the specified time periods.

Exclude Files from a Backup

This step is optional. You can create exclusion rules that use pattern matching to identify directory or file names that are not to be backed up. Files which are typically excluded from backups include temporary files, music, movies and other files which are not essential for business needs.

Use the following steps to create an exclusion rule:
Click here to expand...

1. Go to the **BACKUP > Exclusions** page of the Barracuda Backup web interface. Click **Add an Exclusion**.
2. Fill in the information on the **Add an Exclusion** page:
    - **Exclusion Rule Name** - Enter a descriptive label to identify the exclusion rule.
    - **Add Exclusions to Reports** - Turn on to include exclusions in reports, and turn off if you do not want to include exclusions in the reports.
    - **Apply Recursively to Sub Directories -** Specify whether to apply the exclusion rule recursively to sub directories.
    - **Where to Exclude** - Turn **Apply to All Computers and Data Sources for this Barracuda Backup Server** on to apply the exclusion rule to all computers and data sources for the selected Barracuda Backup Server, or turn off, then expand and select the items to which to apply the exclusion rule.
3. In the **What to Exclude** section, specify what to exclude:
    - From the **Preset Expressions** menu, select the content you want to exclude, for example, **Video files**, then click **Add**.
    - In the **Expressions** field, enter a search string to exclude, for example, ***.mp3**, then click **Add**.
4. Click **Save** at the top of the page to add the exclusion rule.

To edit an existing exclusion rule, go to the **BACKUP > Exclusions** page of the Barracuda Backup web interface, and click **Edit** following the exclusion rule you want to edit. Make the necessary changes, then click **Save**.

To delete an exclusion rule, go to the **BACKUP > Exclusions** page of the Barracuda Backup web interface, and click the **Delete** icon following the exclusion rule you want to remove. Click **OK** to remove the rule.

Create Data Retention Policies

Data is retained based on a traditional grandfather-father-son (daily-weekly-monthly) rotation model. You can specify how long to keep daily, weekly, monthly, and yearly backups by creating data retention policies.
Different retention policies can be created for different sets of data including files, data backed up by the Barracuda Backup Agent (Exchange, SQL, System State), and email messages.

You can create one policy for all of the computers and data sources on a Barracuda Backup Server or multiple policies that each include some subset of the data.

To set retention policies:
Click here to expand...

1. Go to the **BACKUP > Retention Policies** page, click **Add a Retention Policy**, and enter a name to identify the policy.
2. In the **Items to Retain** section, specify the data sources to which the retention policy applies; the **Retention Timeline** section displays. Select a timeline template on which to base your retention policy, or specify your own revision timeline.
3. Select the desired **Removed Files Rule** setting, and click **Save**.

When data is removed according to a retention policy, it is deleted from both the local Barracuda Backup Server and the offsite storage locations. Removed files that have been backed up using Network File Shares Protocol or SSHFS may be retained for a longer period of time, according to the configuration. Otherwise, once your data has been purged, it is gone forever. Purging applies to historic file revisions only; your current data is not impacted by a retention policy.

Check Backup Reports

View reports on an ongoing basis as needed. The **REPORTS > Backup** page contains detailed backup reports. A list of in progress backups displays at the top of the page, and once a backup is complete, a detailed report displays in a table by device. Click **Details** following the report you want to view.

Web Interface

This section describes each page in the Barracuda Backup web interface.

In this Section

- STATUS Page
- BACKUP Page
- RESTORE Page
- REPORTS Page
- SYSTEM Page
- ADMIN Page

STATUS Page

This article refers to firmware version 5.0 and higher, except where noted.

In this article:

- Backup Activity Section
- Storage Efficiency Statistics
- Local Storage
- Transfer History
- Status Indicators

Related Articles

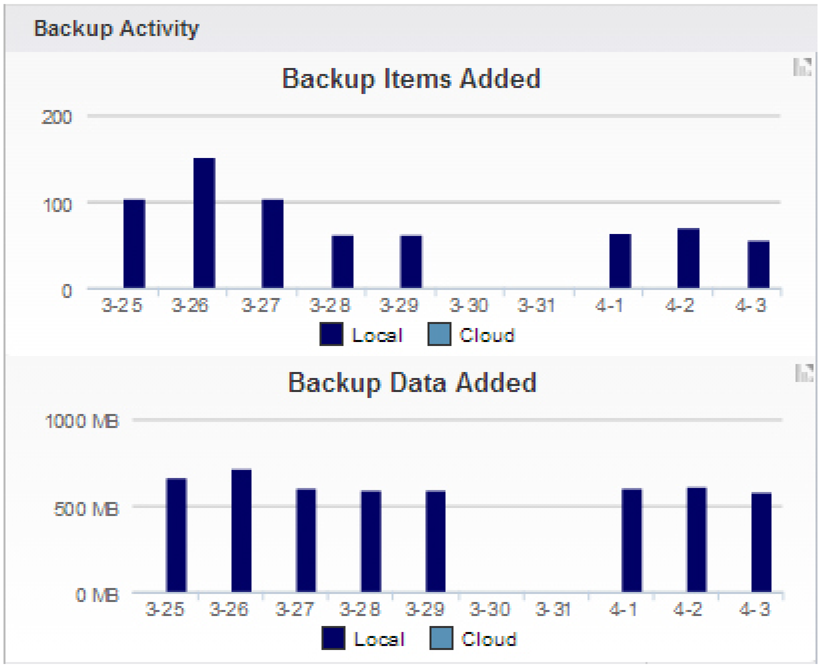
- Advanced Graphs (firmware version 5.3.00 and higher)
- Task Messages (Local UI login)

The **STATUS** page provides an overview of the performance and health of your Barracuda Backup. If you have more than one Barracuda Backup Server linked to your account, you can select a specific server and view its individual statistics. Click on a graph to view a larger display of the data.

> ⓘ **Mobile Access**
>
> You can also view Barracuda Backup Server status using Barracuda Networks Mobile Applications:
>
> - Barracuda Networks iOS Mobile Application for iPhone and iPod Touch
> - Barracuda Networks iOS Mobile Application for iPad

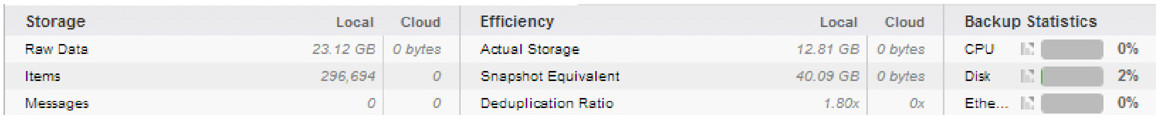
Backup Activity Section

These two graphs displays backup activity for local locations and cloud storage, indicating the size and the number of backup items and data added by date including the number of files and messages backed up:



Storage Efficiency Statistics

This section displays storage efficiency statistics:



Storage	Local	Cloud	Efficiency	Local	Cloud	Backup Statistics	
Raw Data	23.12 GB	0 bytes	Actual Storage	12.81 GB	0 bytes	CPU	0%
Items	296,694	0	Snapshot Equivalent	40.09 GB	0 bytes	Disk	2%
Messages	0	0	Deduplication Ratio	1.80x	0x	Ethe...	0%

Table 1. Storage Efficiency Statistics.

Table Value	Description
Raw Data	Total amount of data sent to Barracuda Backup including revisions.
Items	Total items sent to Barracuda Backup.
Messages	Total messages sent to Barracuda Backup.
Actual Storage	The amount of actual storage space being used.
Snapshot Equivalent	The amount of space that would be required to back up your data based on your retention policies projected over the next three years, without deduplication and compression.
Deduplication Ratio	The overall amount of space savings with deduplication and compression compared to the snapshot equivalent.
Backup Statistics	Displays performance statistics for the Barracuda Backup Servers, including percentage of CPU, disk, and Ethernet usage. Performance statistics displayed in red signify that the value exceeds the normal threshold. These values fluctuate based on the amount of data that is being backed up, but if any setting remains consistently red for a long period of time, contact Barracuda Networks Technical Support.

Local Storage

If you have one Barracuda Backup Server selected in the left pane of the web interface, this table displays the Storage History for that Barracuda Backup Server. View current, historic, and actual data storage size on the local and cloud locations by date.

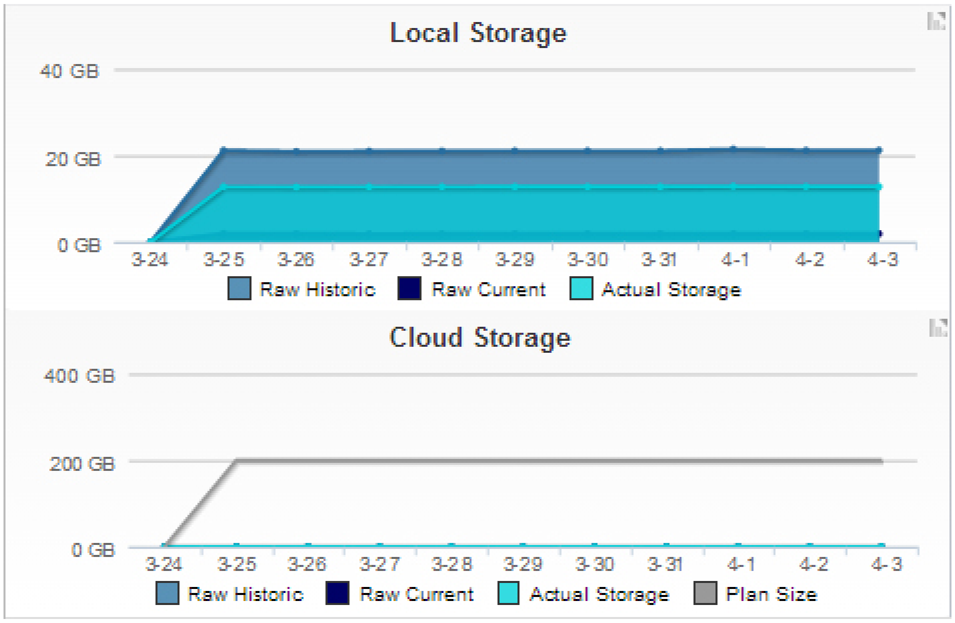


Table 2. Local Storage.

Table Value	Description
For local storage, stored content displays in GB by:	
Raw Current	Represents current content sent to the Barracuda Backup before deduplication processing.
Raw Historic	Represents all content up to the current date that has been sent to the Barracuda Backup.
Actual Storage	Represents the total content currently stored on Barracuda Backup.
For cloud storage, stored content displays in GB by:	
Raw Current	Represents current content sent to the Barracuda Backup before deduplication processing.
Raw Historic	Represents all content up to the current date that has been sent to the Barracuda Backup.
Actual Storage	Represents the total content currently stored on Barracuda Backup.
Plan Size	Indicates total data storage based on your subscription plan size

Transfer History

If you have one Barracuda Backup Server selected in the left pane of the web interface, this table displays efficiency of your data transfer and the size of the file parts yet to be transferred offsite, organized by date, for that Barracuda Backup Server.

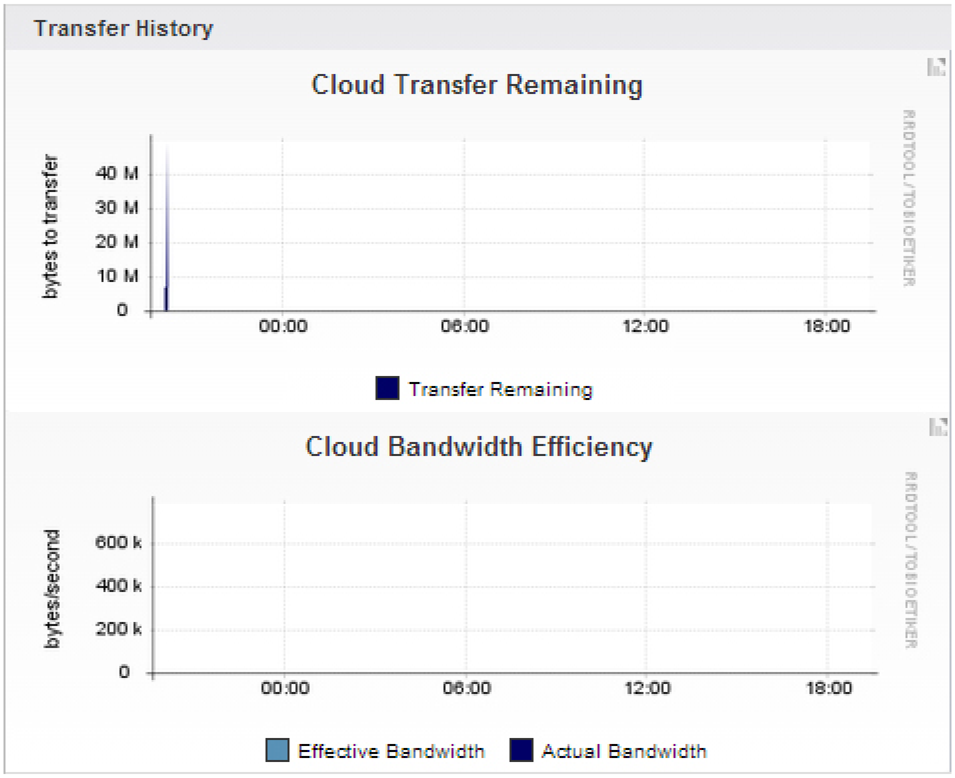
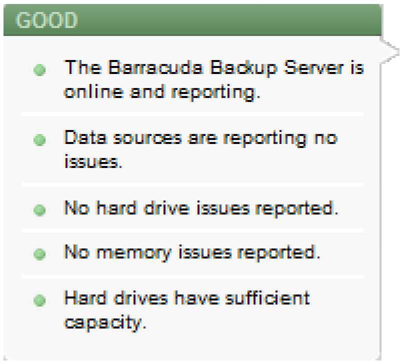

Transfer History
Cloud Transfer Remaining
bytes to transfer
40 M
30 M
20 M
10 M
0
00:00
06:00
12:00
18:00
Transfer Remaining
RRDTOOL / TOBI OETIKER
Cloud Bandwidth Efficiency
bytes/second
600 k
400 k
200 k
0
00:00
06:00
12:00
18:00
Effective Bandwidth
Actual Bandwidth
RRDTOOL / TOBI OETIKER

Table 3. Transfer History.

Table Value	Description
Cloud Transfer Remaining	Displays any content waiting to transfer to the Barracuda Cloud Storage in bytes.
Cloud Bandwidth Efficiency	Represents all content up to the current date that has been sent to the Barracuda Backup based on the maximum data transfer rate of your connection. To limit Internet bandwidth consumption during peak usage times, set rate limits and schedule backups for non-peak hours.
Actual Storage	Displays effective and actual bandwidth efficiency in bytes per second.

Status Indicators

Status indicators for the health of the Barracuda Backup Servers, local and offsite backups, and data sources display in the right pane of the web interface. Green shows that your servers are online and that no errors have been encountered as a result of your backup. Red indicators display when a local server is offline or when errors were generated during a backup. Mouse-over the indicators to see more details:



- The Barracuda Backup Server is online and reporting.
- Data sources are reporting no issues.
- No hard drive issues reported.
- No memory issues reported.
- Hard drives have sufficient capacity.

How to Monitor Backup Status

To check whether a Barracuda Backup Server is operating correctly, select it from the list of Barracuda Backup Servers in the left pane, and click **STATUS**.

The **STATUS** page displays the following Barracuda Backup Server statistics:

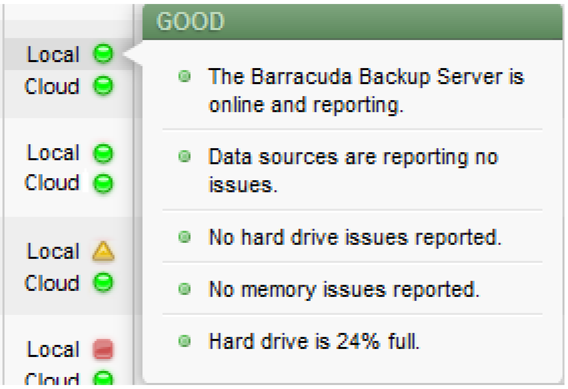
- Backup activity
- Device and backup source status
- Storage, efficiency, and performance statistics
- Storage history for both local and cloud storage
- Transfer History

Click on a graph to view a closeup of the details and immediately update the data displayed in the graph.

The Transfer History section displays the amount of bytes remaining to be transferred. If there is a large amount of data there (80 GB or more), there are a number of things to check, all under the **BACKUP** tab:

- Adjust the rate limit
- Check the amount of data being backed up nightly to ensure the Barracuda Backup Server is doing transaction log backups for Exchange and SQL
- Check retention policies to ensure that too much historic data is not being transferred

To check the status of all of your Barracuda Backup Servers at once, click **Backup** at the top of the left pane, and go to the **STATUS** page. If the status of a Barracuda Backup Server is yellow or red, there is a problem with connectivity or the health of the Barracuda Backup Server. If you mouse over the various indicators, the condition details display:



- The Barracuda Backup Server is online and reporting.
- Data sources are reporting no issues.
- No hard drive issues reported.
- No memory issues reported.
- Hard drive is 24% full.

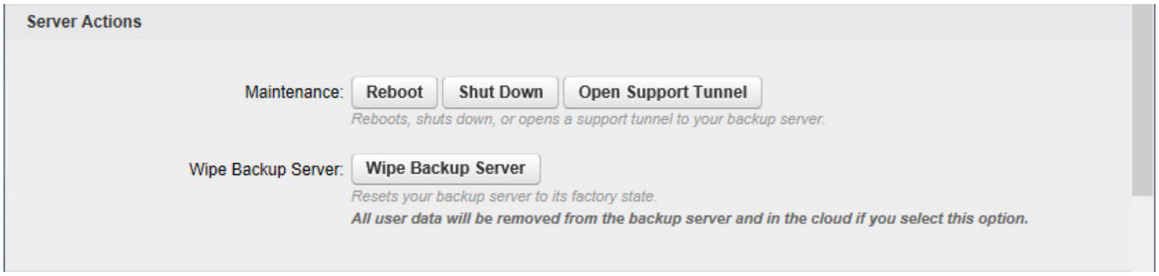
Additional information can be found on the Reports page.

How to Unlink a Barracuda Backup Server

This article refers to Barracuda Backup firmware version 3.0 or higher.

If you need to link a Barracuda Backup Server to a different account, use the following steps to unlink the Barracuda Backup Server from the current account:

1. Enter the Barracuda Backup Server IP address to log in to the local web interface.
2. Go to the **STATUS** page, and in the **Server Actions** section, click **Wipe Backup Server**:

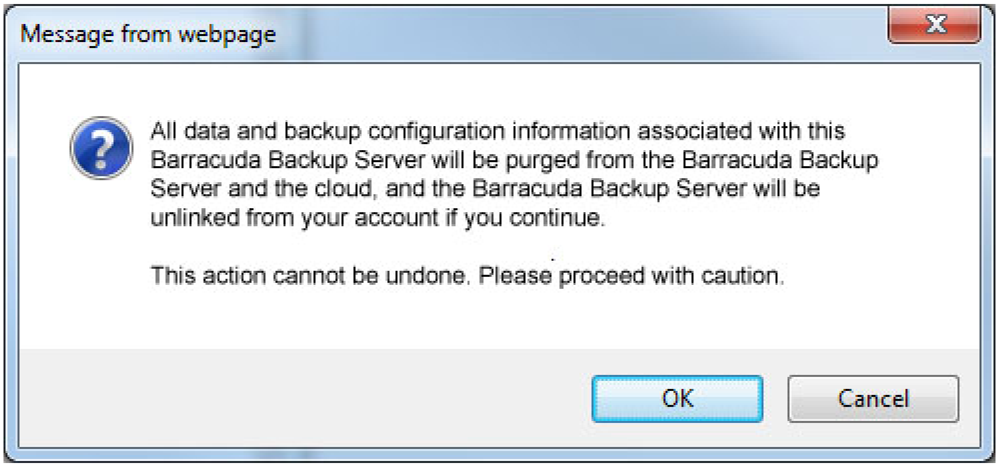

Server Actions
Maintenance:
Reboot
Shut Down
Open Support Tunnel
Wipe Backup Server:
Wipe Backup Server

Reboots, shuts down, or opens a support tunnel to your backup server.

Resets your backup server to its factory state.

All user data will be removed from the backup server and in the cloud if you select this option.

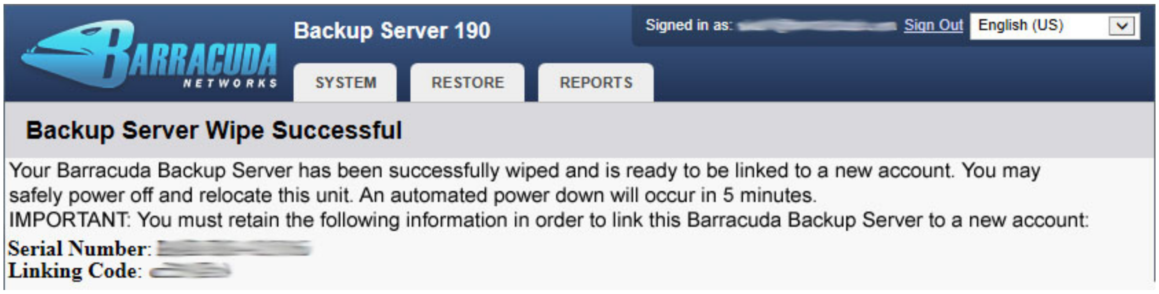
3. The message **Wipe Started Successfully** displays in the web interface. Once the unlinking process is in progress, a warning message displays:


Message from webpage
OK
Cancel

All data and backup configuration information associated with this Barracuda Backup Server will be purged from the Barracuda Backup Server and the cloud, and the Barracuda Backup Server will be unlinked from your account if you continue.

This action cannot be undone. Please proceed with caution.

4. Click **OK** to complete the unlinking process. Once the Barracuda Backup Server is unlinked from the account, the **Backup Server Wipe Successful** page displays, including the Serial Number and Linking Code:


BARRACUDA NETWORKS
Backup Server 190
Signed in as: [redacted]
Sign Out
English (US)
SYSTEM
RESTORE
REPORTS

Backup Server Wipe Successful

Your Barracuda Backup Server has been successfully wiped and is ready to be linked to a new account. You may safely power off and relocate this unit. An automated power down will occur in 5 minutes.
IMPORTANT: You must retain the following information in order to link this Barracuda Backup Server to a new account:
Serial Number: [redacted]
Linking Code: [redacted]

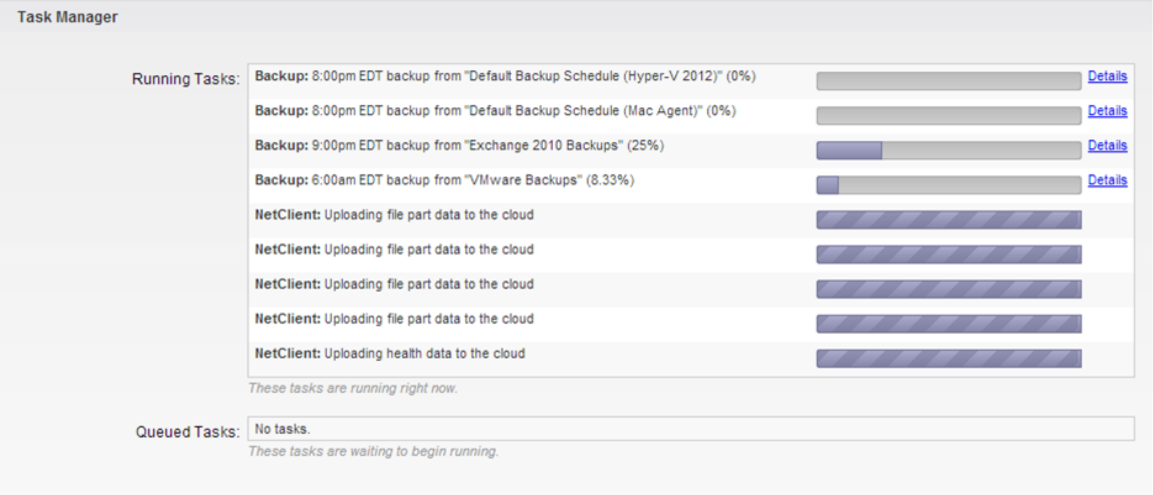
5. Make note of the serial number and linking code. You can now link the Barracuda Backup Server to a new account. For details, see How to Link a Barracuda Backup Server as a User or Reseller.

Task Messages

This article refers to Barracuda Backup firmware version 5.0 or higher.

Use the following steps to view the **STATUS** page in the Barracuda Backup *local web interface*:

1. Open a web browser, and enter the Barracuda Backup Server IP address.
2. Log in to the Barracuda Backup local web interface; the **System** page displays.
3. In the **Task Manager** section, **Running Tasks** and **Queued Tasks** display:



Task Manager

Running Tasks:

Backup: 8:00pm EDT backup from "Default Backup Schedule (Hyper-V 2012)" (0%) Details
Backup: 8:00pm EDT backup from "Default Backup Schedule (Mac Agent)" (0%) Details
Backup: 9:00pm EDT backup from "Exchange 2010 Backups" (25%) Details
Backup: 6:00am EDT backup from "VMware Backups" (8.33%) Details
NetClient: Uploading file part data to the cloud
NetClient: Uploading file part data to the cloud
NetClient: Uploading file part data to the cloud
NetClient: Uploading file part data to the cloud
NetClient: Uploading health data to the cloud

These tasks are running right now.

Queued Tasks: No tasks.

These tasks are waiting to begin running.

4. Click **Details** to toggle additional information on or off.

Processes and Services

The following table describes the processes and services that display on the **SYSTEM** page:

Backup	Daemon responsible for performing backup functions.
Restore	Daemon responsible for performing restore functions.
Netclient	Process used to replicate data to another location.
Netserver	Process that receives data from netclient for box-to-box replication.
Purger	Deletes files that fall outside of the retention policy, and shares removed from the configuration.

BACKUP Page

This article refers to firmware version 5.0 and higher.

Use the **BACKUP** page to manage how data is backed up. From this page you can back up data locally then replicate the data offsite with complete control over where data is stored. Barracuda Backup offers a full line of servers for local backup that can be configured to support offsite replication to the cloud, private locations, or a combination of both.

Related Articles

- How to Increase Backup Performance
- Understanding Source-Based Deduplication

Location	Description	Related Articles

BACKUP > Sources	Use this page to configure where data is backed up and in what manner: - Identify systems to be backed up - Select the type of data to be backed up - Specify where data is backed up	- How to Configure Backups - Data Backup Tasks - Backing Up Data Sources - Barracuda Backup Agent - Barracuda Linux Backup Agent
BACKUP > Replication	Configure backup data replication to one or more other Barracuda Backup Servers. From this page you can view: - **Target List** - Displays where data from the selected Barracuda Backup Server is sent - **Source List** - Displays a list of devices sending data to the selected Barracuda backup Server	- Getting Started with Replication - Configuring a Replication Destination - How to Temporarily Disable a Destination - How to Manage the Data Queue - How to Configure Barracuda Backup
BACKUP > Schedules	Once you configure computers and data sources, use this page to create backup schedules.	- Backup Schedules
BACKUP > Rate Limit	Rate limits control the data replication rate to Barracuda Cloud Storage or other offsite storage locations. Use this page to limit Internet bandwidth consumption during peak usage times, and schedule backups for non-peak hours.	- Setting Up Rate Limits
BACKUP > Exclusions	Create exclusion rules that use pattern matching to identify directory or file names you do not want to back up. Files which are typically excluded from backups include temporary files, music, movies and other files which are not essential for business needs.	- Backup Exclusions
BACKUP > Retention Policies	Specify how long to keep daily, weekly, monthly, and yearly backups by creating data retention policies. Different retention policies can be created for different sets of data including files, data backed up by the Barracuda Backup Agent (Exchange, SQL, System State), and email messages. You can create one policy for all of the computers and data sources on a Barracuda Backup Server or multiple policies that each include some subset of the data.	- Backup Retention Policies - Creating Effective Retention Policies

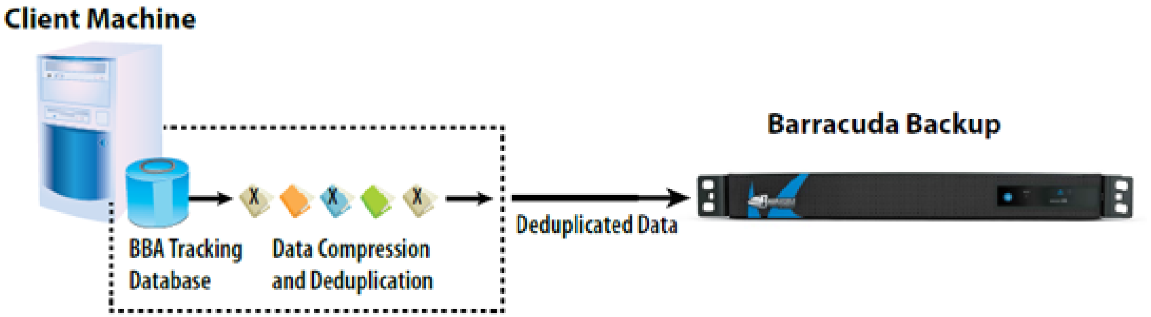
BACKUP > Watched Files	Use this page to add files to watch on a particular Barracuda Backup Server. File watch rules are used to monitor and send email alerts when specified files have not been changed often enough or appear smaller than expected. ⓘ The seldomly used Watched Files feature has been deprecated in firmware versions 5.2, and will not be supported for new Barracuda Backup Servers. Note that existing Watched File Rules will continue to function as expected.	- Setting Up Watched Files

Understanding Source-Based Deduplication

Barracuda's source deduplication method deduplicates local data on the client-side, removing redundancies from the data before transmission, and then sends that data to the Barracuda Backup Server in deduplicated form, minimizing LAN bandwidth and data sent to the local server.

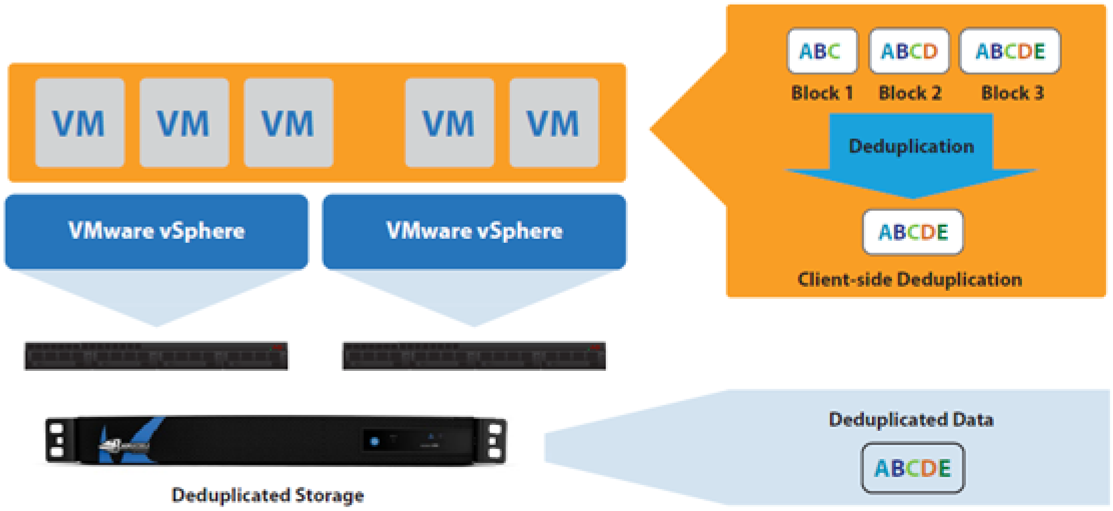
Source deduplication is implemented through the Barracuda Backup Agent. During Agent installation, a small database is created on the server to keep track of data chunks so only unique data is compressed and sent to the Barracuda Backup appliance for processing, reducing network traffic and the backup window, as shown in Figure 1.

Figure 1. Source Deduplication.



For VMware backups, Barracuda leverages VMware’s vStorage APIs for Data Protection (VADP) to back up virtual disks, utilizing Changed Block Tracking (CBT) to send only unique chunks to the Barracuda Backup Server, as shown in Figure 2.

Figure 2. Changed Block Tracking.


VM
VM
VM
VM
VM
VMware vSphere
VMware vSphere
ABC
ABCD
ABCDE
Block 1
Block 2
Block 3
Deduplication
ABCDE
Client-side Deduplication
Deduplicated Data
ABCDE
Deduplicated Storage

With source deduplication, organizations running Microsoft Hyper-V also benefit from Barracuda Backup. The Barracuda Backup Agent reduces the backup window by minimizing the amount of data sent to the Barracuda Backup Server by deduplicating the VHD files on the host server.

Backing Up Data Sources

In this Section

- Microsoft Exchange Server and Exchange Server DAG
- Microsoft Hyper-V
- Microsoft SQL Server
- VMware
- How to Back Up Microsoft Active Directory
- How to Back Up and Restore a Microsoft SharePoint SQL Database
- Understanding IBM Domino Server Backup
- How to Configure GroupWise Message-Level Backups
- How to Set Up a Root Account to Back Up Macintosh OS X
- How to Back Up Linux/UNIX Data Using SSHFS
- Understanding Changed Block Tracking on Virtual Machines
- How to Enable Changed Block Tracking through the Barracuda Backup Web Interface
- How to Back Up Network Addressable Storage - NAS
- How to Back Up FirstClass Mail
- How to Back Up NFS Mounts with the Barracuda Backup Agent (Linux)
- How to Back Up NSS Mounts with the Barracuda Backup Agent (Linux)

Related Articles

- Barracuda Backup Agent (Windows)
- Barracuda Backup Agent (Linux)
- Monitoring Windows System Performance During Backup

Microsoft Exchange Server and Exchange Server DAG

In this Section

- How to Set Up Microsoft Exchange Server 2003, 2007, 2010 Message-Level Backups
- Understanding Microsoft Exchange Server 2003 and 2007 Storage Group Backup
- How to Back Up Microsoft Exchange Server 2010 DAG
- How to Back Up Microsoft Exchange Server 2010 DAG Passive Database

- How to Back Up Microsoft Exchange Server 2013
- How to Set Up Microsoft Exchange Server 2013 Message-Level Backup

How to Set Up Microsoft Exchange Server 2003, 2007, 2010 Message-Level Backups

> This article refers to Barracuda Backup firmware version 4.3 and higher, and Microsoft® Exchange Server 2003, 2007, and 2010.
>
> For details on setting up Microsoft Exchange Server 2013 message-level backup, refer to the article How to Set Up Microsoft Exchange Server 2013 Message-Level Backup.

In this article:

- Requirements
- Barracuda Backup Server DNS Settings
- Step 1. Determine the Exchange Server Version and Build
    - Exchange Server 2003 Version and Build
    - Exchange Server 2007 Version and Build
    - Exchange Server 2010 Version and Build
- Step 2. Set Up Your Exchange Server
    - Set Up Exchange Server 2003 (Service Pack 1 or Above)
    - Set Up Exchange Server 2007 (Service Pack 1 or Above)
    - Set Up Exchange Server 2010
- Step 3. Add the Exchange Server to the Barracuda Backup Web Interface

Related Articles

- Backing Up Data Sources
- Configuring Backups
- Restoring Exchange and GroupWise Messages
- Exchange 2013 Message-Level Backup

Additional Resource

- The Barracuda Networks Knowledgebase Solution #00003906

> **Message-Level Backup**
> Message-level backup provides a quick way to restore single email messages to the original location or to an alternate mailbox. Message-level backup is not intended to be a disaster recovery option for your Microsoft Exchange environment. The Barracuda Backup Agent (Windows) allows you to back up the entire Exchange Information Store and should be used for disaster protection.

Requirements

You must be running one of the following Microsoft Exchange Servers:

- Microsoft Exchange Server 2003 Service Pack 1 or above; *or*
- Microsoft Exchange Server 2007 Service Pack 1 or above; *or*
- Microsoft Exchange Server 2010

In addition, you must have the following:

- Outlook Web Access (with WebDAV enabled)
- Primary and Secondary DNS setting on the Barracuda Backup Server must be DNS servers which participate in Active Directory
- Service account for access that has an Exchange mailbox and SMTP address

Barracuda Backup Server DNS Settings

For Exchange messagelevel backups to work properly, it is *very* important that DNS is set up correctly. DNS servers on the Barracuda Backup Server must be DNS servers that participate in Active Directory. The simplest way to determine which DNS servers to use is to use the IP addresses of your Active Directory Domain Controllers.

Step 1. Determine the Exchange Server Version and Build

Before setting up your Exchange Server, it is important to know what version, including the build number, is running to verify your Exchange

Server is running the minimum requirement for Exchange messagelevel backups. Locate the version and build number for your Exchange Server, then refer to the Microsoft knowledgebase article Build numbers and release dates for Exchange Server to verify you are running the correct version, and if applicable, service pack:

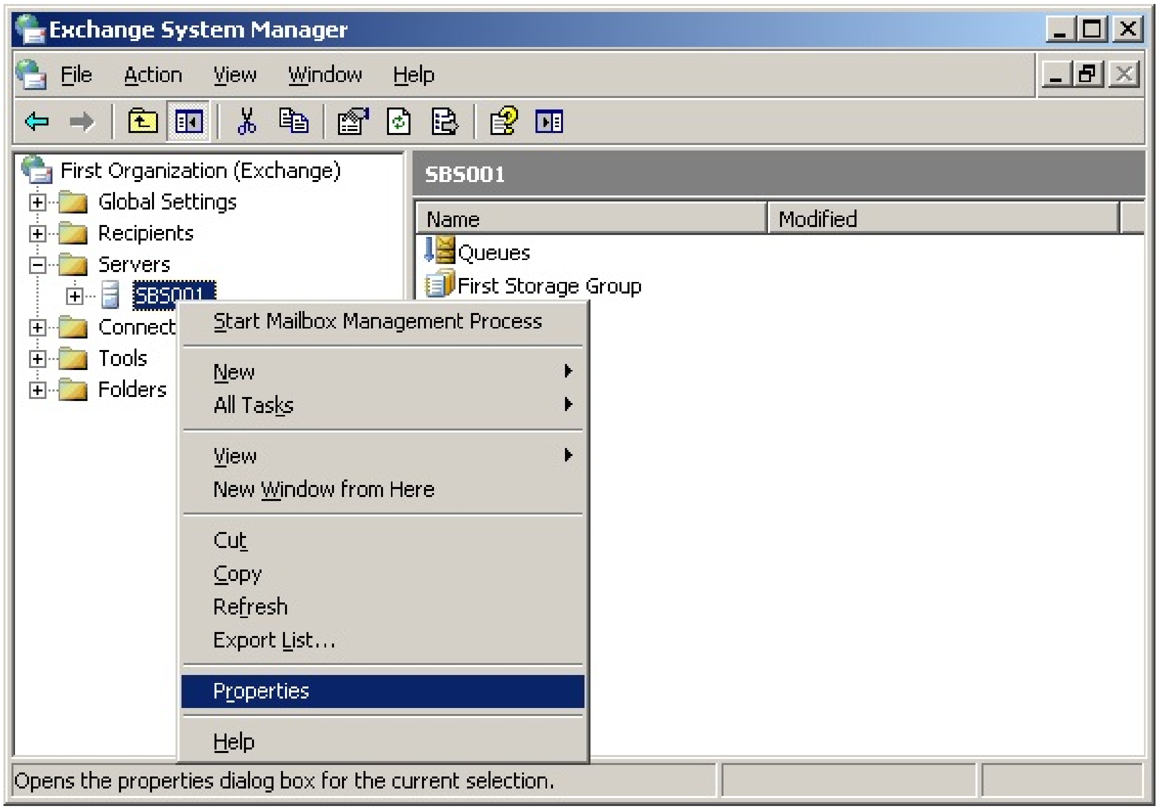
- Exchange Server 2003 Version and Build
- Exchange Server 2007 Version and Build
- Exchange Server 2010 Version and Build

Exchange Server 2003 Version and Build

Use the following steps to determine the version and service pack number on Exchange Server 2003.

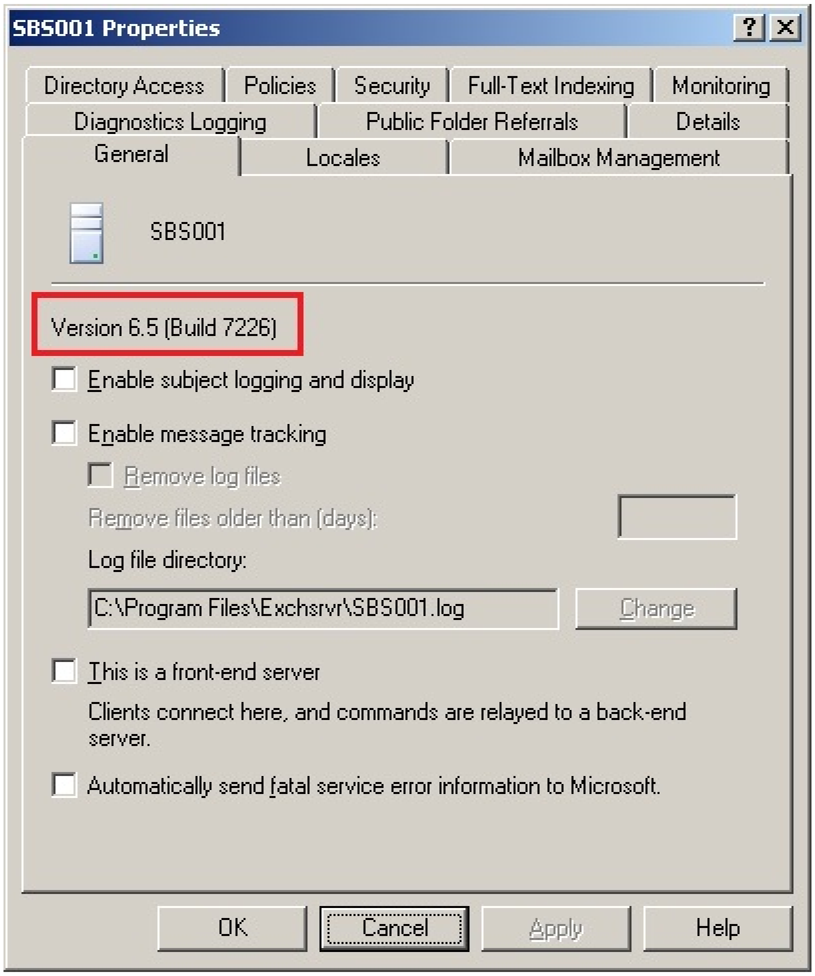
Click here to expand...

1. Open the Exchange System Manager on the Exchange Server, expand **Servers** folder, right-click on the server name, and click **Properties**:


Exchange System Manager
File
Action
View
Window
Help
First Organization (Exchange)
Global Settings
Recipients
Servers
SBS001
Connect
Tools
Folders
SBS001
Name
Modified
Queues
First Storage Group
Start Mailbox Management Process
New
All Tasks
View
New Window from Here
Cut
Copy
Refresh
Export List...
Properties
Help

Opens the properties dialog box for the current selection.

2. The version and build number display in the **General** tab:


SBS001 Properties
Directory Access
Policies
Security
Full-Text Indexing
Monitoring
Diagnostics Logging
Public Folder Referrals
Details
General
Locales
Mailbox Management
Change
OK
Cancel
Apply
Help

SBS001

Version 6.5 (Build 7226)

☐ Enable subject logging and display

☐ Enable message tracking

☐ Remove log files

Remove files older than (days):

Log file directory:

C:\Program Files\Exchsrvr\SBS001.log

☐ This is a front-end server

Clients connect here, and commands are relayed to a back-end server.

☐ Automatically send fatal service error information to Microsoft.

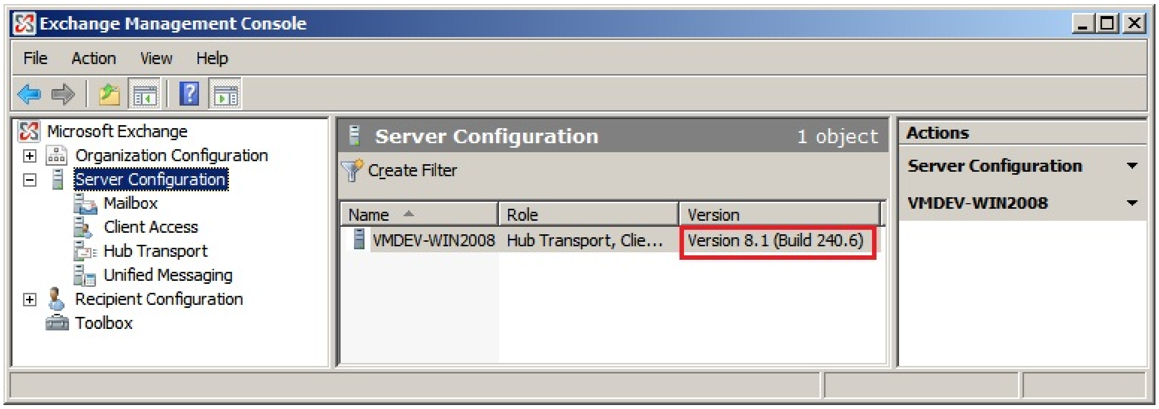
3. Open the Microsoft knowledgebase article Build numbers and release dates for Exchange Server to determine the version and service pack level the Exchange Server is running; the minimum requirement for Exchange Server 2003 with Service Pack 1 is Version 6.5, Build 7226.
4. Go to Step 2.

Exchange Server 2007 Version and Build

Use the following steps to determine the version and service pack number on Exchange Server 2007.

Click here to expand...

1. Open the Exchange System Manager on the Exchange Server, and click **Server Configuration:**


Exchange Management Console
File
Action
View
Help
Microsoft Exchange
Organization Configuration
Server Configuration
Mailbox
Client Access
Hub Transport
Unified Messaging
Recipient Configuration
Toolbox
Create Filter
Actions
Server Configuration
VMDEV-WIN2008

Server Configuration 1 object

Name	Role	Version
VMDEV-WIN2008	Hub Transport, Clie...	Version 8.1 (Build 240.6)

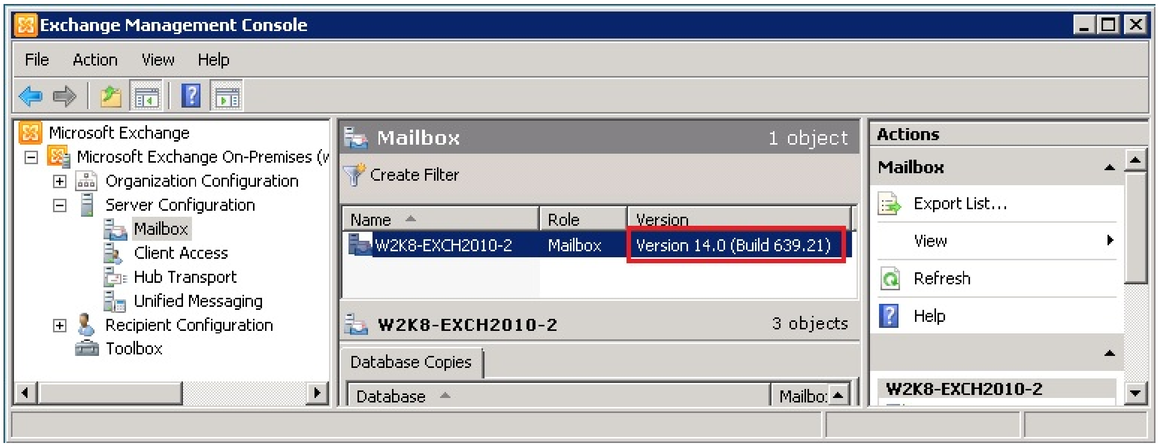
2. Open the Microsoft knowledgebase article Build numbers and release dates for Exchange Server to determine the version and service pack level the Exchange Server is running.
3. Go to step 2.

Exchange Server 2010 Version and Build

If you are running Exchange Server 2010, use the following steps to determine the version number.

Click here to expand...

1. Open the Exchange System Manager on the Exchange Server, expand **Server Configuration**, and click **Mailbox**; the Exchange Server version displays in the center pane:


Exchange Management Console
File
Action
View
Help
Microsoft Exchange
Microsoft Exchange On-Premises (v
Organization Configuration
Server Configuration
Mailbox
Client Access
Hub Transport
Unified Messaging
Recipient Configuration
Toolbox
Mailbox
1 object
Create Filter
Name
Role
Version
W2K8-EXCH2010-2
Mailbox
Version 14.0 (Build 639.21)
W2K8-EXCH2010-2
3 objects
Database Copies
Database
Mailbo:
Actions
Mailbox
Export List...
View
Refresh
Help
W2K8-EXCH2010-2

2. Open the Microsoft knowledgebase article Build numbers and release dates for Exchange Server to determine the version the Exchange Server is running.
3. Go to Step 2.

Step 2. Set Up Your Exchange Server

Select the applicable steps based on your Exchange Server version:

- Setting Up Exchange Server 2003
- Setting Up Exchange Server 2007
- Setting Up Exchange Server 2010

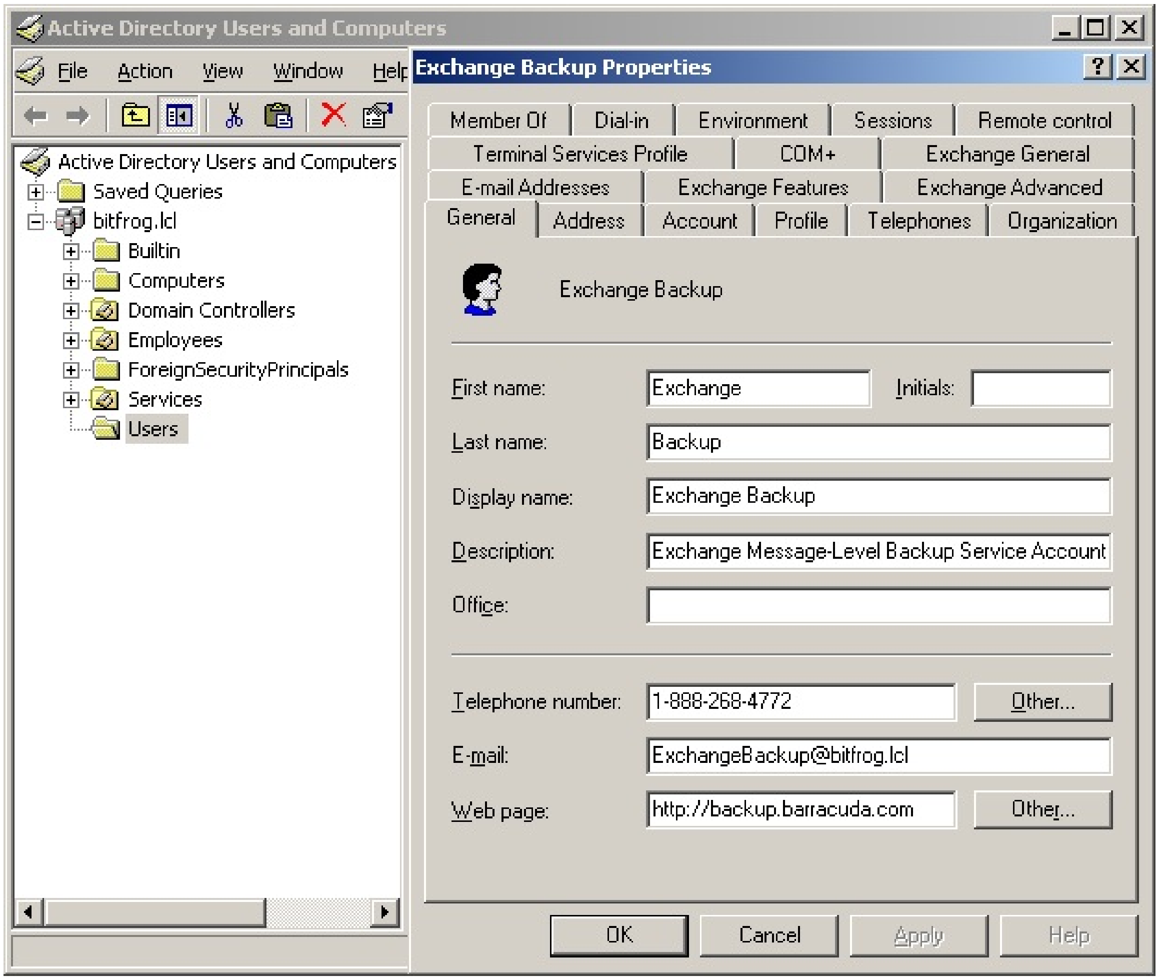
Set Up Exchange Server 2003 (Service Pack 1 or Above)

Use the following steps to set up your Exchange Server 2003 for message-level backups.

Click here to expand...

1. Create an account to be used by Barracuda Backup to access emails in each mailbox:

> **Service Type Account**
> It is *strongly* recommended that you use a service type account and *not* your administrator account to prevent inherited deny permissions from causing issues. This service account requires an Exchange mailbox and SMTP address and must be a member of either the **Enterprise Admins** group or **Domain Admins** group.

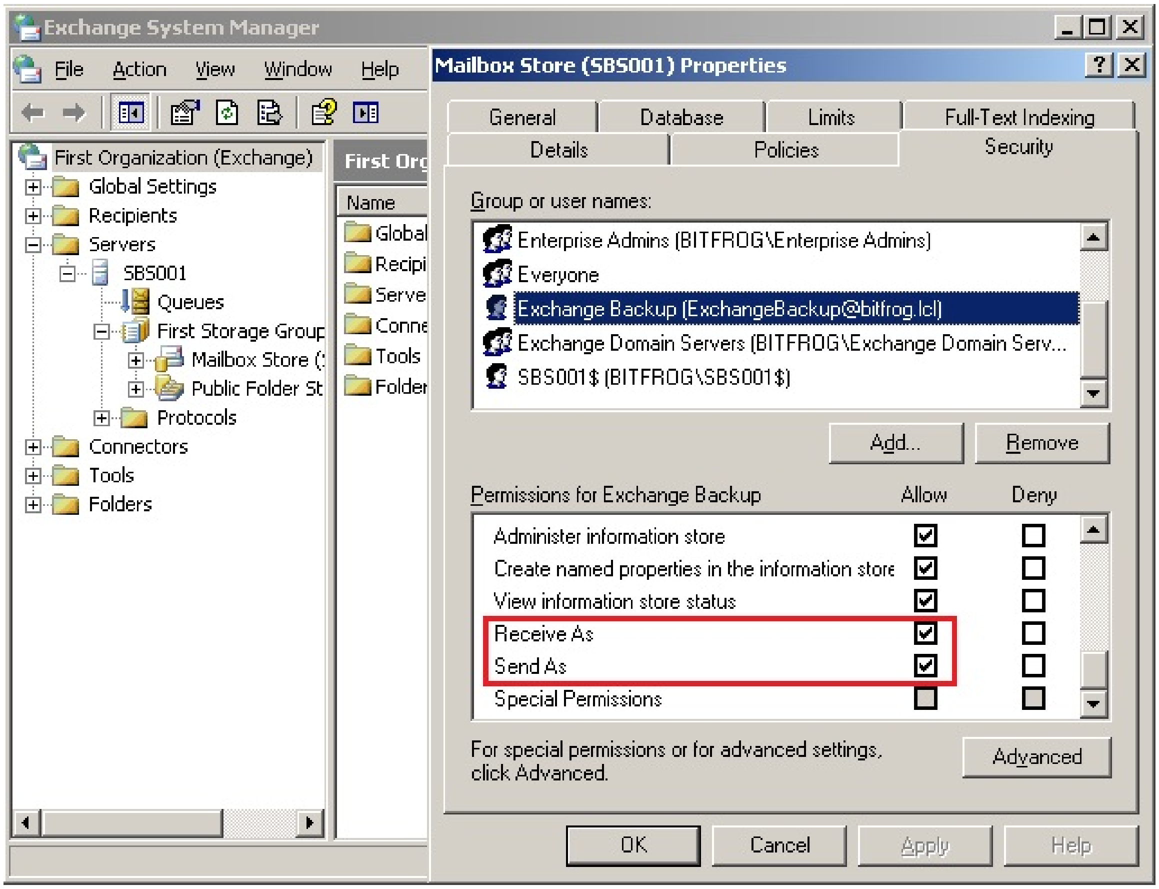

Active Directory Users and Computers
File
Action
View
Window
Help
Active Directory Users and Computers
Saved Queries
bitfrog.lcl
Builtin
Computers
Domain Controllers
Employees
ForeignSecurityPrincipals
Services
Users
Member Of
Dial-in
Environment
Sessions
Remote control
Terminal Services Profile
COM+
Exchange General
E-mail Addresses
Exchange Features
Exchange Advanced
General
Address
Account
Profile
Telephones
Organization
Other...
Other...
OK
Cancel
Apply
Help

Exchange Backup Properties

Exchange Backup

First name: Exchange
Initials:
Last name: Backup
Display name: Exchange Backup
Description: Exchange Message-Level Backup Service Account
Office:
Telephone number: 1-888-268-4772
E-mail: ExchangeBackup@bitfrog.lcl
Web page: http://backup.barracuda.com

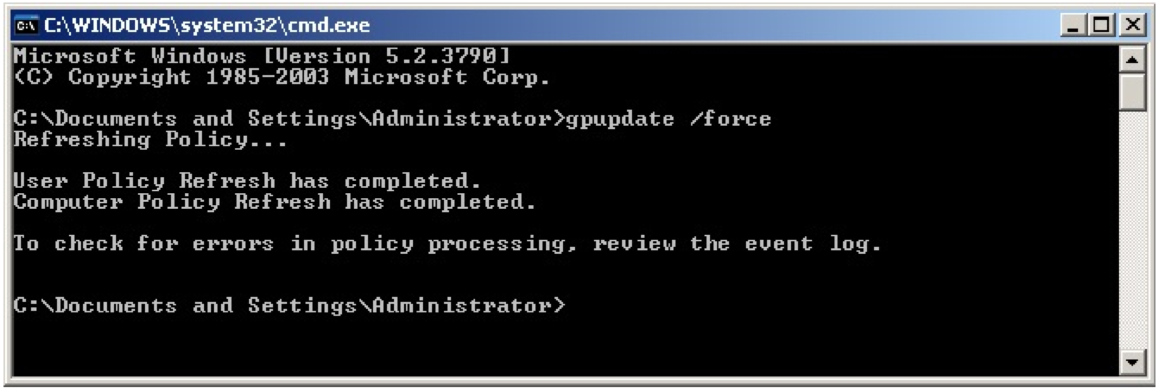
2. Assign the service account permissions on the Storage Groups on your Exchange Server.
3. Open the Exchange System Manager, click **Servers**, and then expand your server.
4. Right-click **First Storage Group**, and click **Properties** on the Mailbox Store in the first storage group.
5. Click on the **Security** tab, and add your backup service account to the **Group or user names** section of the **Mailbox Store Properties**; click on the backup service account name.
6. In **Permissions for Exchange Backup**, turn on **Allow** for both **Receive As** and **Send As** permissions:


Exchange System Manager
File Action View Window Help
First Organization (Exchange)
Global Settings
Recipients
Servers
SBS001
Queues
First Storage Group
Mailbox Store (
Public Folder St
Protocols
Connectors
Tools
Folders
First Org
Name
Global
Recipi
Serve
Conne
Tools
Folder
Mailbox Store (SBS001) Properties
General
Database
Limits
Full-Text Indexing
Details
Policies
Security
Group or user names:
Add...
Remove
For special permissions or for advanced settings, click Advanced.
Advanced
OK
Cancel
Apply
Help

Enterprise Admins (BITFROG\Enterprise Admins)
Everyone
Exchange Backup (ExchangeBackup@bitfrog.lcl)
Exchange Domain Servers (BITFROG\Exchange Domain Serv...
SBS001$ (BITFROG\SBS001$)

Permissions for Exchange Backup	Allow	Deny
Administer information store	☑	☐
Create named properties in the information store	☑	☐
View information store status	☑	☐
Receive As	☑	☐
Send As	☑	☐
Special Permissions	☐	☐

7. Depending on replication policies and Exchange Server activity, it may be helpful to perform a group policy update on the Exchange Server to help replicate permissions. To do so, run the following command from the command line:
`gpupdate /force`


C:\WINDOWS\system32\cmd.exe

```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>gpupdate /force
Refreshing Policy...

User Policy Refresh has completed.
Computer Policy Refresh has completed.

To check for errors in policy processing, review the event log.


C:\Documents and Settings\Administrator>
```

8. Go to Step 3 to complete the set up.

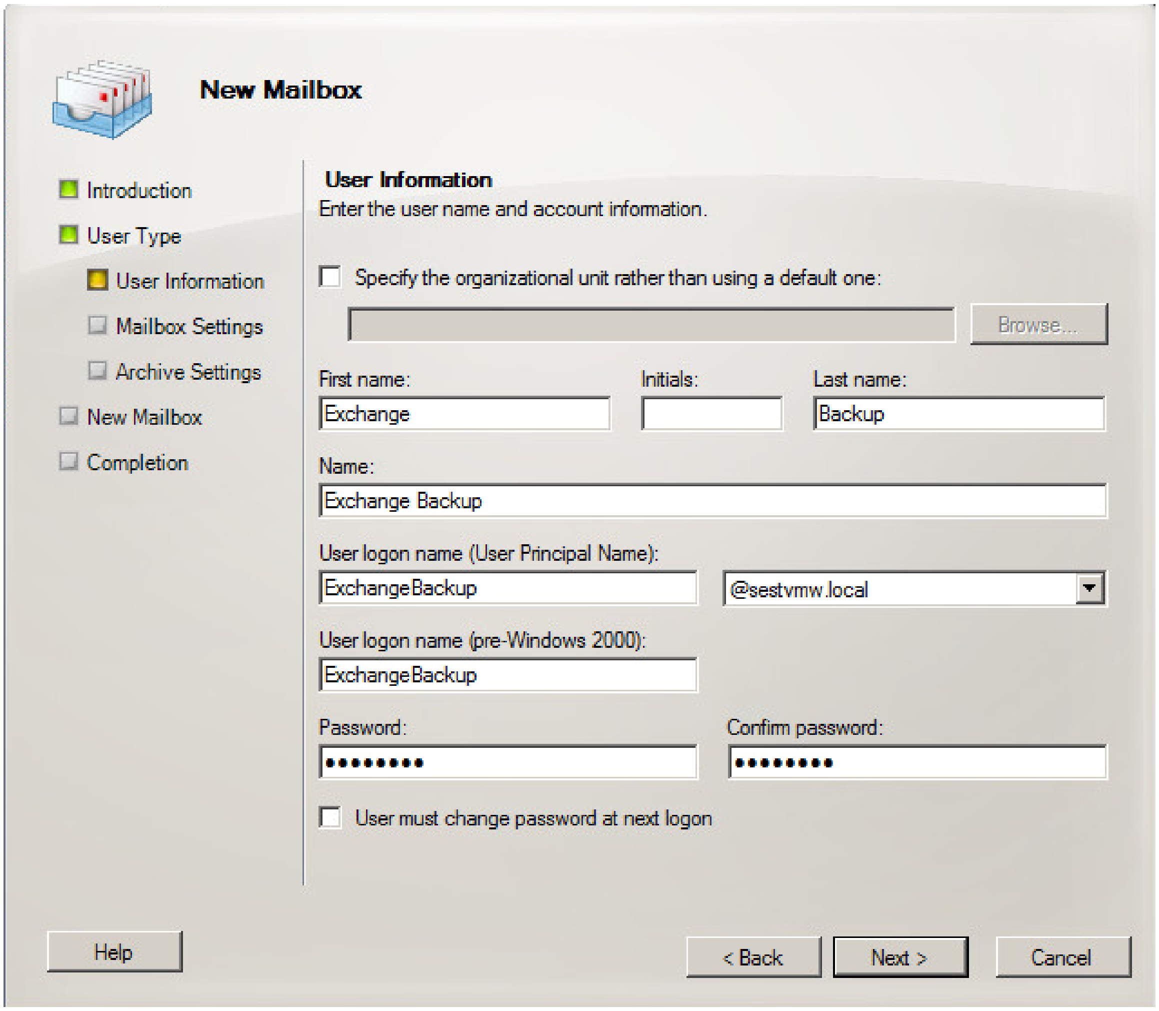
Set Up Exchange Server 2007 (Service Pack 1 or Above)

Use the following steps to set up your Exchange Server 2007 to do message-level backups.

Click here to expand...

1. Create an account to be used by Barracuda Backup to access emails in each mailbox:

> **Service Type Account**
> It is *strongly* recommended that you use a service type account and *not* your administrator account to prevent inherited deny permissions from causing issues. This service account requires an Exchange mailbox and SMTP address and must be a member of one of the following groups: **Exchange View Only Administrators**, **Exchange Organization Administrators**, **Enterprise Admins**, or **Domain Admins**.


New Mailbox
Introduction
User Type
User Information
Mailbox Settings
Archive Settings
New Mailbox
Completion
Browse...
Help
< Back
Next >
Cancel

User Information

Enter the user name and account information.

☐ Specify the organizational unit rather than using a default one:

First name: Exchange

Initials:

Last name: Backup

Name: Exchange Backup

User logon name (User Principal Name): ExchangeBackup @sestvmw.local

User logon name (pre-Windows 2000): ExchangeBackup

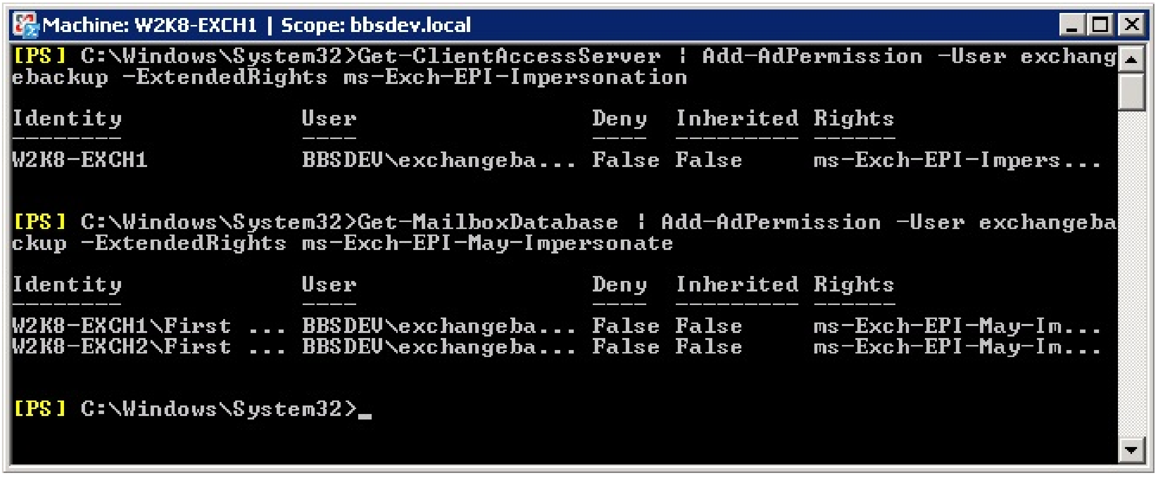
Password: ••••••••

Confirm password: ••••••••

☐ User must change password at next logon

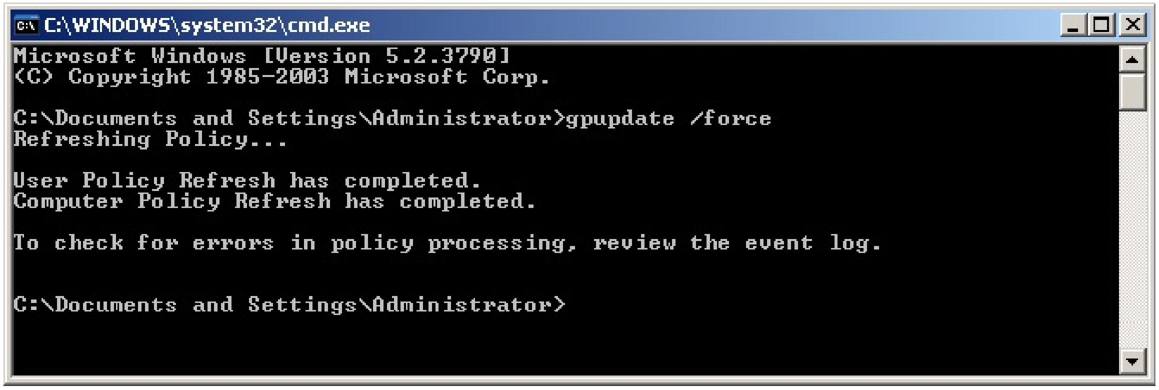
2. Assign the service account permissions to the Mailbox Databases on your Exchange server.
3. Open the Exchange Management Shell, and run the following command replacing *`<ServiceAccount>`* with the Service Account username:

```
Get-ClientAccessServer | Add-AdPermission -User <ServiceAccount> -ExtendedRights
ms-Exch-EPI-Impersonation
Get-MailboxDatabase | Add-AdPermission -User <ServiceAccount> -ExtendedRights
ms-Exch-EPI-May-Impersonate
```


Machine: W2K8-EXCH1 | Scope: bbsdev.local

```
[PS] C:\Windows\System32>Get-ClientAccessServer | Add-AdPermission -User exchang
ebackup -ExtendedRights ms-Exch-EPI-Impersonation

Identity             User                 Deny  Inherited Rights
--------             ----                 ----  --------- ------
W2K8-EXCH1           BBSDEV\exchangeba... False False     ms-Exch-EPI-Impers...


[PS] C:\Windows\System32>Get-MailboxDatabase | Add-AdPermission -User exchangeba
ckup -ExtendedRights ms-Exch-EPI-May-Impersonate

Identity             User                 Deny  Inherited Rights
--------             ----                 ----  --------- ------
W2K8-EXCH1\First ... BBSDEV\exchangeba... False False     ms-Exch-EPI-May-Im...
W2K8-EXCH2\First ... BBSDEV\exchangeba... False False     ms-Exch-EPI-May-Im...


[PS] C:\Windows\System32>_
```

4. Depending on replication policies and Exchange Server activity, it may be helpful to perform a group policy update on the Exchange Server to help replicate permissions. To do so, run the following command from the command line:
`gpupdate /force`



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>gpupdate /force
Refreshing Policy...

User Policy Refresh has completed.
Computer Policy Refresh has completed.

To check for errors in policy processing, review the event log.


C:\Documents and Settings\Administrator>
```

5. Go to Step 3 to complete the set up.

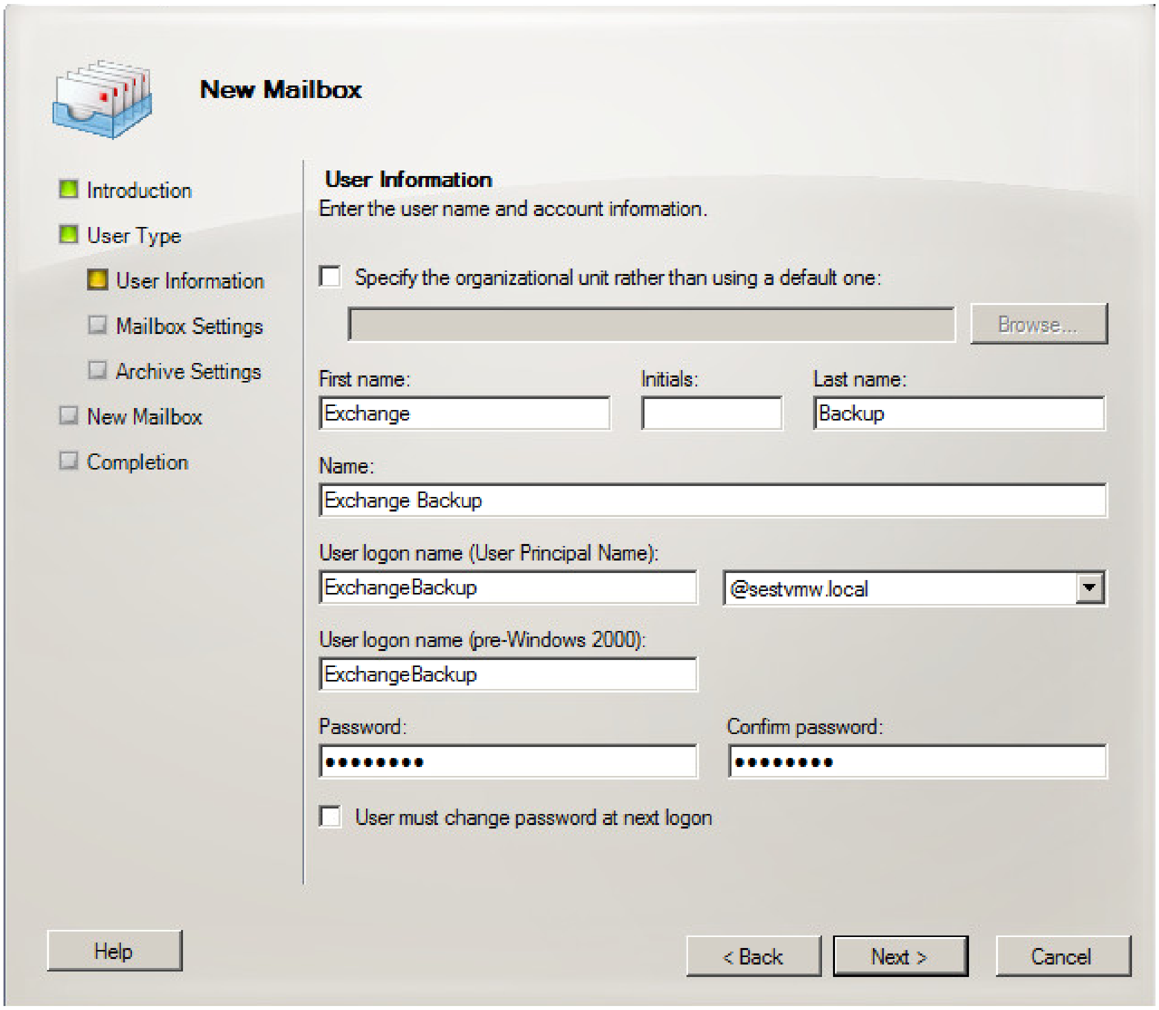
Set Up Exchange Server 2010

Use the following steps to set up your Exchange Server 2010 to do message-level backups.

Click here to expand...

1. Create an account to be used by Barracuda Backup to access emails in each mailbox:

> **Service Type Account**
> It is *strongly* recommended that you use a service type account and *not* your administrator account to prevent inherited deny permissions from causing issues. This service account requires an Exchange mailbox and SMTP address and must be a member of one of the **Domain Users** group; adding the service account to any administrative groups may cause issues with access to user mailboxes.



New Mailbox

User Information

Enter the user name and account information.

☐ Specify the organizational unit rather than using a default one:

First name: Exchange

Initials:

Last name: Backup

Name: Exchange Backup

User logon name (User Principal Name): ExchangeBackup @sestvmw.local

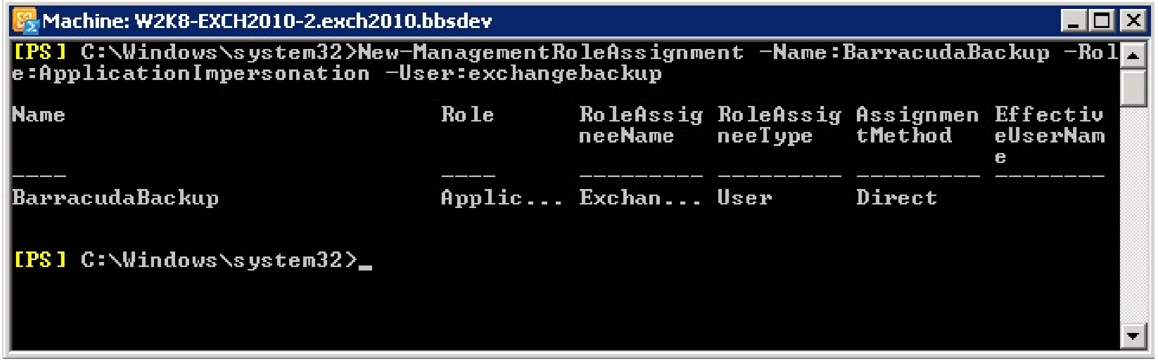
User logon name (pre-Windows 2000): ExchangeBackup

Password: ••••••••

Confirm password: ••••••••

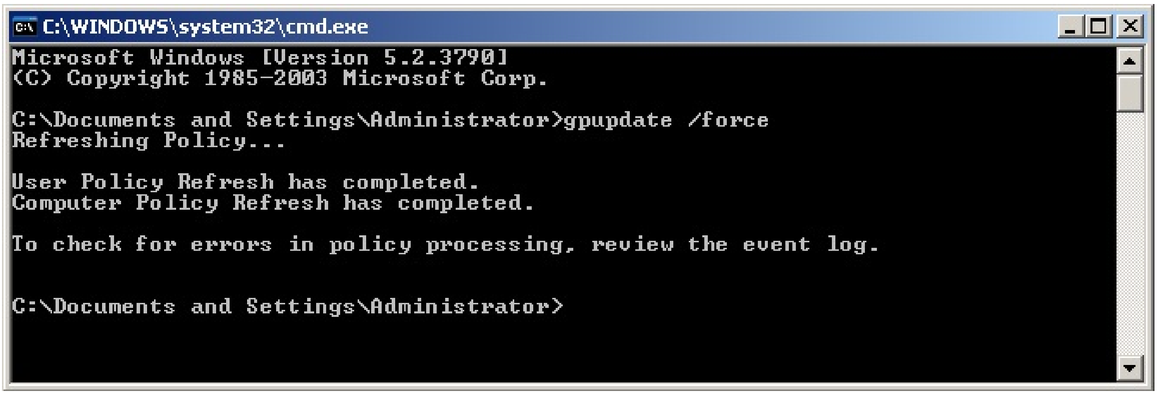
☐ User must change password at next logon

2. To assign the service account impersonation rights for Exchange, open the Exchange Management Shell, and run the following command, replacing *`<ServiceAccount>`* with the Service Account username:



```
[PS] C:\Windows\system32>New-ManagementRoleAssignment -Name:BarracudaBackup -Rol
e:ApplicationImpersonation -User:exchangebackup

Name                           Role       RoleAssig RoleAssig Assignmen Effectiv
                                          neeName   neeType   tMethod   eUserNam
                                                                        e
----                           ----       --------- --------- --------- --------
BarracudaBackup                Applic...  Exchan... User      Direct


[PS] C:\Windows\system32>_
```

3. Depending on replication policies and Exchange Serer activity, it may be helpful to perform a group policy update on the Exchange Server to help replicate permissions. To do so, run the following command from the command line:
`gpupdate /force`



```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>gpupdate /force
Refreshing Policy...

User Policy Refresh has completed.
Computer Policy Refresh has completed.

To check for errors in policy processing, review the event log.


C:\Documents and Settings\Administrator>
```

4. Go to Step 3 to complete the set up.

Step 3. Add the Exchange Server to the Barracuda Backup Web Interface

Once you set up your Exchange installation to allow the Barracuda Backup Server to access it, use the following steps to add the Exchange Server to the web interface:

1. Log in to Barracuda Backup, and go to on the **BACKUP > Sources** page.
2. Click **Add Computer**; in the **Add Computer** page, add the Exchange Server details including the hostname or IP address, and click **Save**.
3. In the **Add Data Source** page, select **Message-Level Backup (Exchange)** as the **Data Type**. In the **Message-Level Backup (Exchange) Information** section, select the Exchange Server version, and enter the Server details.

> **Base DN Field**
> The **Base DN** field is optional; enter the Base Distinguished Name only if directed to do so by Barracuda Networks Technical Support.

4. Click **Test Exchange Connectivity** to verify the Server credentials.
5. If the connectivity test returns OK, you can now select the mailboxes you want to back up in the **Mailbox Selection** section.
6. Click **Save** to add the data source.

Understanding Microsoft Exchange Server 2003 and 2007 Storage Group Backup

This article refers to Barracuda Backup firmware version 3.1 or higher, and Microsoft® Exchange Server 2003 or 2007.

In this article:

- Exchange Storage Group
- Backup Process
    - Operation 1. Cache is Flushed and Checkpoint is

  Halted
- Operation 2. Back Up Database Files
- Operation 3. Transaction logs
- Operation 4. Log Files are Truncated
- Operation 5. Backup Operation Complete

Related Articles

- Restore an Exchange 2007 Database
- Restore an Exchange 2003 Database by Overwriting Existing Database
- Restore an Exchange 2003 Database using a Recovery Storage Group

Exchange Storage Group

The Barracuda Backup Agent for Microsoft Exchange Server provides a full backup of the Exchange storage group. An Exchange storage group is a logical container for your email database and its associated system and transaction log files.

Microsoft Exchange uses transaction logging to commit new and changed data to the database, and to ensure that records of the transactions exist if a store is damaged between backups. The Exchange storage group, and its associated transaction logs, is the most important data to back up on your Exchange Server to ensure your email database is available in the event it becomes damaged or unrecoverable. If you must rebuild a server, you can use the latest transaction log files plus the last full backup to recover your database.

The Barracuda Backup Agent for Microsoft Exchange Server backs up and restores the entire storage group; it allows for the storage group to be restored to a storage group or to an alternate Microsoft Exchange Server.

Backup Process

Several important operations occur at the start of the Exchange storage group backup process. Here is the overview of the backup process:

Operation 1. Cache is Flushed and Checkpoint is Halted

When a full backup operation is initialized, the Exchange Server Extensible Storage Engine (ESE) first flushes its cache to disk and halts the checkpoint. The checkpoint cannot advance until the backup operation is complete. It is important to note that when a partial backup such as a differential, incremental, or copy backup runs, ESE allows the checkpoint to advance because the backup operation does not touch the databases.

Operation 2. Back Up Database Files

The backup application uses backup API calls to pass a list of databases to ESE for back up. ESE sends the backup application chunks of database pages in sequential order, and performs a checksum on each page. The backup operation is terminated if an error is encountered.

> ⓘ When a database is backed up using the Exchange streaming backup API, each page in the database is read in turn, and the checksum integrity of each page is verified. Additionally, transaction log file checksum integrity is confirmed before they are backed up.

Operation 3. Transaction logs

ESE stores the transaction logs to the backup set, and halts the checkpoint at the beginning of the backup. To back up the log files, the backup application uses the appropriate API call to request a list of log files (and patch files, if applicable) from ESE. When ESE receives this call, it closes the current log file, saves the file as the next log generation in a sequential list, and opens a new `E0n.log` file where *n* represents the storage group instance of the log file.

- In the case of a full backup, ESE then returns a list of log files to the backup application; this list starts with the current log generation in which the checkpoint was halted, and ends with the log generation that ESE just closed (i.e., `E0n.log` minus 1).
- In the case of an incremental or differential backup, ESE returns a list beginning with the oldest log generation on disk and ending with the most recently closed log generation. Using this list, the backup application can open file handles to the log files and copy them to the backup set. During this operation, ESE ensures that no log generation is missing from the sequence passed to the backup application.

Operation 4. Log Files are Truncated

Once the log files are stored to the backup set, they are no longer needed on disk. During full and incremental backup operations, ESE truncates the log files on disk once transaction log back up is completed. The lower of either the checkpoint log generation or the log generation listed in the database header for the current full backup determines which log files ESE truncates.

Operation 5. Backup Operation Complete

After the log files are truncated, the backup operation is complete and the backup application closes the backup set. ESE returns to normal database-engine operations and permits the checkpoint to advance.

How to Back Up Microsoft Exchange Server 2010 DAG

This article refers to Barracuda Backup firmware 5.1 and higher, and Microsoft Exchange Server 2010 DAG.

Install the Barracuda Backup Agent

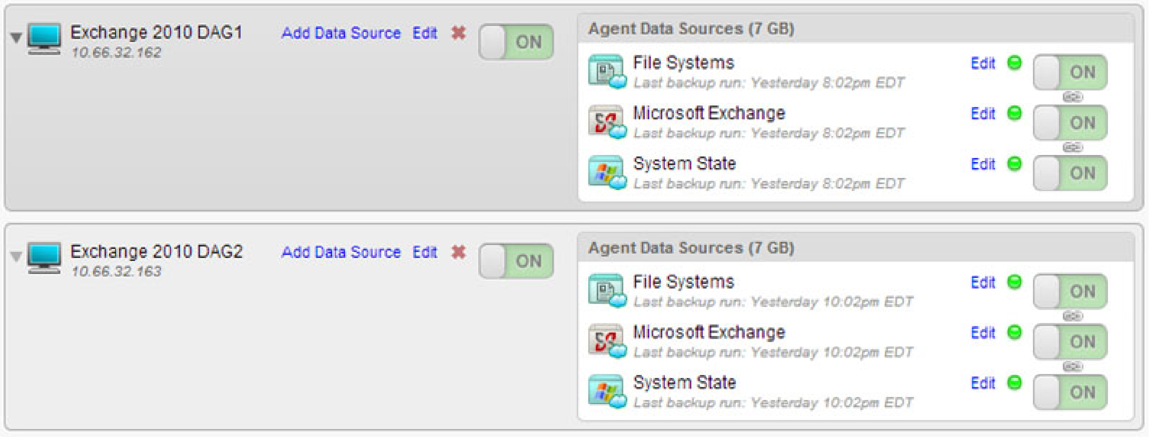
Use the following steps to install the Barracuda Backup Agent (Windows) on all Exchange Servers configured in DAG:

1. Log in to Barracuda Backup, and select the associated Barracuda Backup Server in the left pane.
2. Go to the **SYSTEM > Software Downloads** page.
3. Download and install the Barracuda Backup Agent (Windows) on all Exchange Servers configured in DAG.

Set Up the Exchange Servers

Use the following steps to set up an Exchange Server 2010 DAG backup on the Barracuda Backup Server:

1. Log in to Barracuda Backup, and select the associated Barracuda Backup Server in the left pane.
2. Go to the **BACKUP > Sources** page, and click **Add Computer** to identify the system.
3. Add the Exchange Server with the proper hostname or IP address and description.
4. Select **Microsoft Windows** as the **Computer Type**, and click **Save**.
5. In the **Add Data Source** page, select **Barracuda Agent Software** as the **Data Type**, and click **Test Software Connectivity** to verify the Barracuda Backup Server can communicate with the installed Agent.
6. In the **Item Selection** section, choose to back up all items or specified items (Exchange Databases).
7. Click **Save**. The Exchange Server is added as a data source:


Exchange 2010 DAG1
10.66.32.162
Add Data Source
Edit
ON
Agent Data Sources (7 GB)
File Systems
Last backup run: Yesterday 8:02pm EDT
Edit
ON
Microsoft Exchange
Last backup run: Yesterday 8:02pm EDT
Edit
ON
System State
Last backup run: Yesterday 8:02pm EDT
Edit
ON
Exchange 2010 DAG2
10.66.32.163
Add Data Source
Edit
ON
Agent Data Sources (7 GB)
File Systems
Last backup run: Yesterday 10:02pm EDT
Edit
ON
Microsoft Exchange
Last backup run: Yesterday 10:02pm EDT
Edit
ON
System State
Last backup run: Yesterday 10:02pm EDT
Edit
ON

8. Repeat steps 2 through 7 for each Exchange Server configured in DAG.

How to Back Up Microsoft Exchange Server 2010 DAG Passive Database

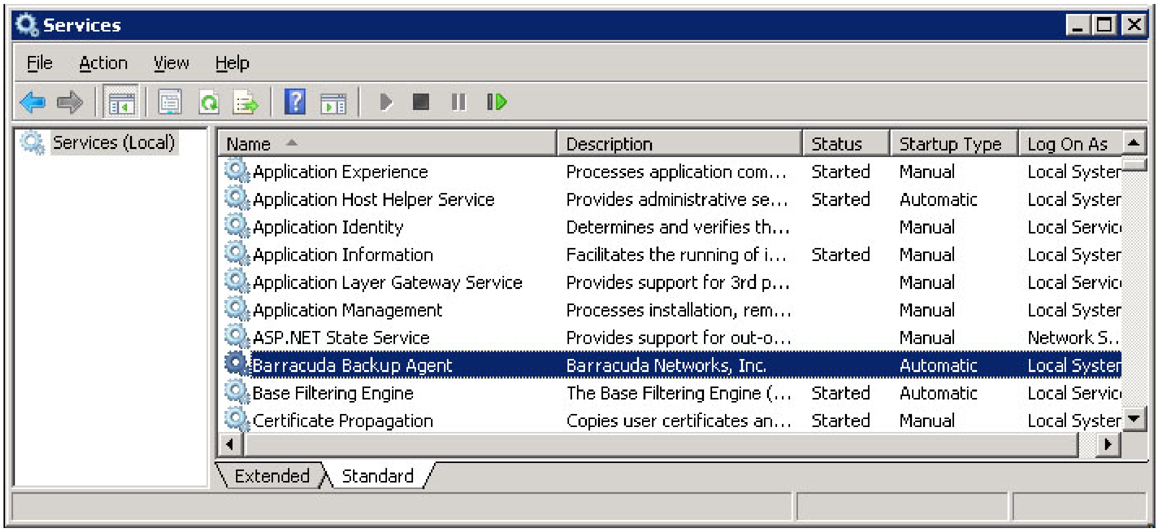
This article refers to Barracuda Backup firmware version 5.0 or higher, and Microsoft Exchange Server 2010 in a Database Availability Group (DAG). This article assumes that you have the Barracuda Backup Agent (Windows) installed on the Exchange Server.

You must complete both Step 1 and Step 2 to back up the passive database.

Step 1. Configure the Barracuda Backup Agent

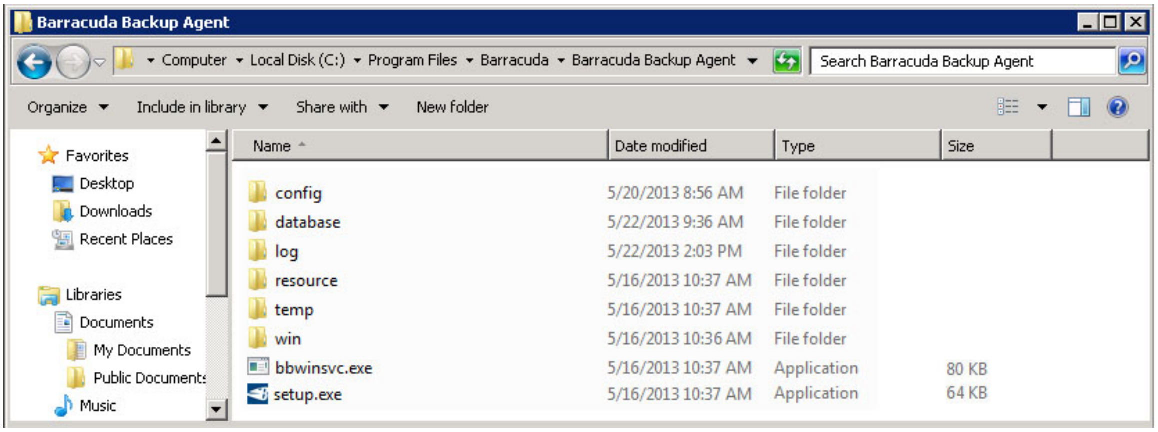
Use this section to configure the Barracuda Backup Agent (Windows) to detect passive databases.

1. Log in to the Exchange Server where the passive database to be backed up resides.
2. Go to **Start > Administrative Tools > Services** to open the Services console.
3. Right-click the **Barracuda Backup Agent** service, and click **Stop**:


Services
File
Action
View
Help
Services (Local)
Extended
Standard

Name	Description	Status	Startup Type	Log On As
Application Experience	Processes application com...	Started	Manual	Local Syster
Application Host Helper Service	Provides administrative se...	Started	Automatic	Local Syster
Application Identity	Determines and verifies th...		Manual	Local Servic
Application Information	Facilitates the running of i...	Started	Manual	Local Syster
Application Layer Gateway Service	Provides support for 3rd p...		Manual	Local Servic
Application Management	Processes installation, rem...		Manual	Local Syster
ASP.NET State Service	Provides support for out-o...		Manual	Network S...
Barracuda Backup Agent	Barracuda Networks, Inc.		Automatic	Local Syster
Base Filtering Engine	The Base Filtering Engine (...	Started	Automatic	Local Servic
Certificate Propagation	Copies user certificates an...	Started	Manual	Local Syster

4. On the Exchange Server, navigate to the Barracuda Backup Agent installation directory; the default location is **C:\Program Files\Barracuda\Barracuda Backup Agent\config**:

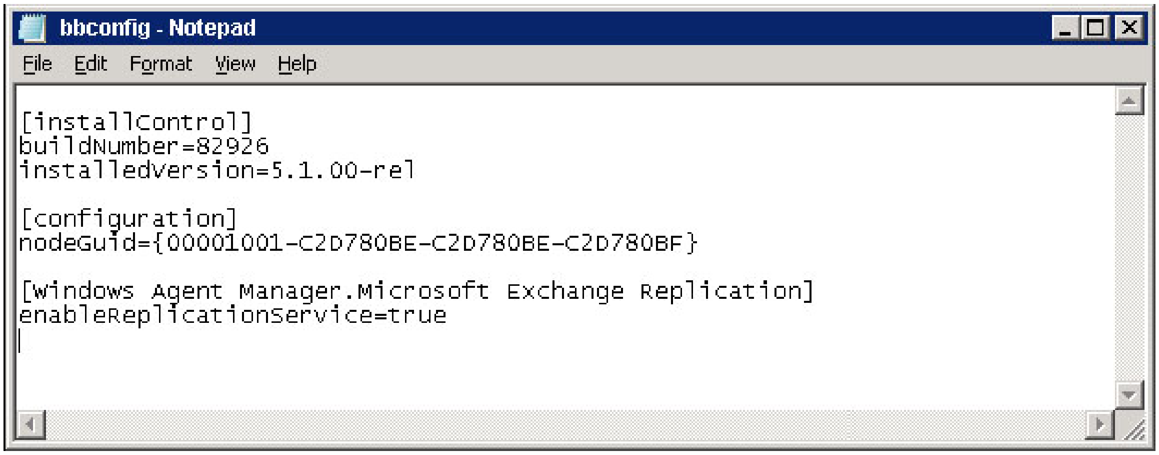

Barracuda Backup Agent
Computer ▸ Local Disk (C:) ▸ Program Files ▸ Barracuda ▸ Barracuda Backup Agent
Search Barracuda Backup Agent
Organize
Include in library
Share with
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
My Documents
Public Documents
Music

Name	Date modified	Type	Size
config	5/20/2013 8:56 AM	File folder	
database	5/22/2013 9:36 AM	File folder	
log	5/22/2013 2:03 PM	File folder	
resource	5/16/2013 10:37 AM	File folder	
temp	5/16/2013 10:37 AM	File folder	
win	5/16/2013 10:36 AM	File folder	
bbwinsvc.exe	5/16/2013 10:37 AM	Application	80 KB
setup.exe	5/16/2013 10:37 AM	Application	64 KB

5. Open the **config** folder, and open **bbconfig.ini** file in **Notepad**.
6. Add the following content beneath the configuration section:

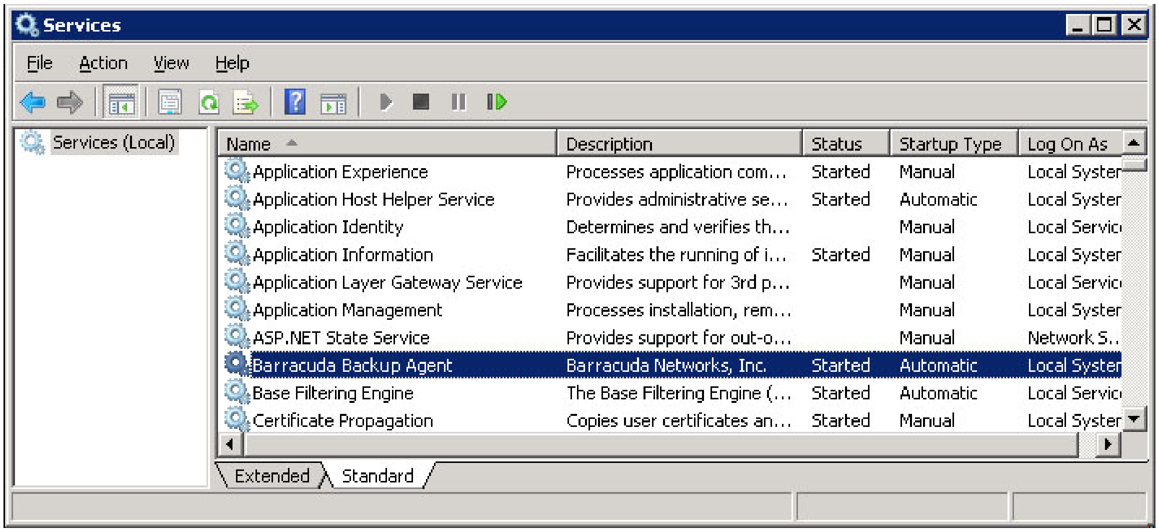
```
[Windows Agent Manager.Microsoft Exchange Replication]
```

`enableReplicationService=true`


bbconfig - Notepad
File Edit Format View Help

```
[installControl]
buildNumber=82926
installedversion=5.1.00-rel

[configuration]
nodeGuid={00001001-C2D780BE-C2D780BE-C2D780BF}

[Windows Agent Manager.Microsoft Exchange Replication]
enableReplicationService=true
```

7. Save the file and close **Notepad**.
8. In the Services Console, right-click the **Barracuda Backup Agent** service, and click **Start** to restart the service:

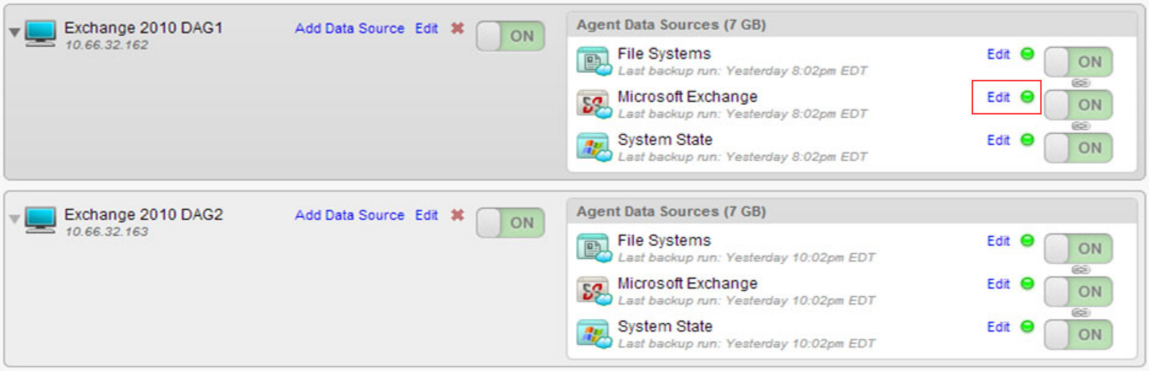

Services
File Action View Help
Services (Local)
Extended
Standard

Name	Description	Status	Startup Type	Log On As
Application Experience	Processes application com…	Started	Manual	Local Syster
Application Host Helper Service	Provides administrative se…	Started	Automatic	Local Syster
Application Identity	Determines and verifies th…		Manual	Local Servic
Application Information	Facilitates the running of i…	Started	Manual	Local Syster
Application Layer Gateway Service	Provides support for 3rd p…		Manual	Local Servic
Application Management	Processes installation, rem…		Manual	Local Syster
ASP.NET State Service	Provides support for out-o…		Manual	Network S…
Barracuda Backup Agent	Barracuda Networks, Inc.	Started	Automatic	Local Syster
Base Filtering Engine	The Base Filtering Engine (…	Started	Automatic	Local Servic
Certificate Propagation	Copies user certificates an…	Started	Manual	Local Syster

Step 2. Configure the Data Source

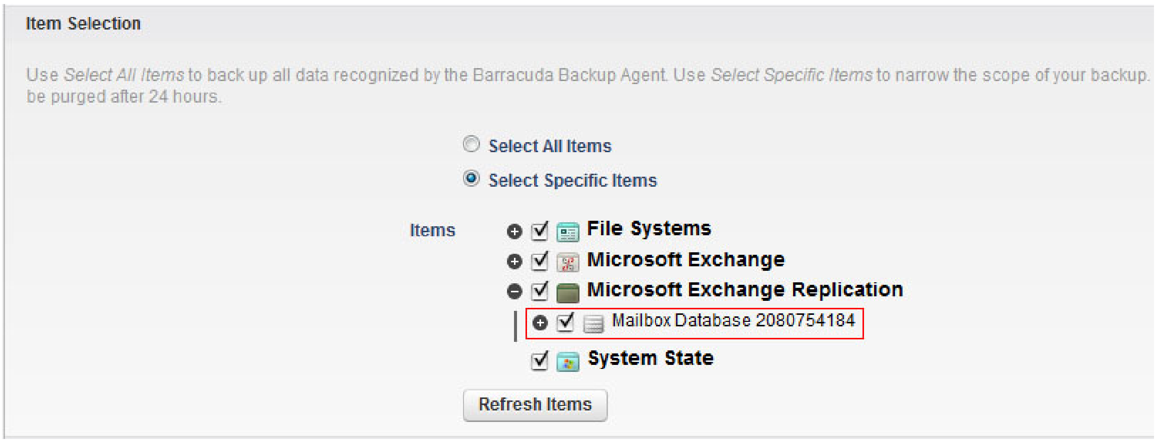
Use this section to configure data sources on the Barracuda Backup Server.

1. Log in to the Barracuda Backup web interface, and select the associated Barracuda Backup Server in the left pane.
2. Go to the **BACKUP > Sources** page, and locate the Exchange Server data sources.
3. Click **Edit** to the right of the Microsoft Exchange Server containing the passive database to be backed up:


Exchange 2010 DAG1
10.66.32.162
Add Data Source
Edit
ON
Agent Data Sources (7 GB)
File Systems
Last backup run: Yesterday 8:02pm EDT
Edit
ON
Microsoft Exchange
Last backup run: Yesterday 8:02pm EDT
Edit
ON
System State
Last backup run: Yesterday 8:02pm EDT
Edit
ON
Exchange 2010 DAG2
10.66.32.163
Add Data Source
Edit
ON
Agent Data Sources (7 GB)
File Systems
Last backup run: Yesterday 10:02pm EDT
Edit
ON
Microsoft Exchange
Last backup run: Yesterday 10:02pm EDT
Edit
ON
System State
Last backup run: Yesterday 10:02pm EDT
Edit
ON

4. In the **Edit Data Source** page, in the **Item Selection** section, click **Select Specific Items**; the **Microsoft Exchange Replication** item displays. Expand **Microsoft Exchange Replication** to access the passive

database:

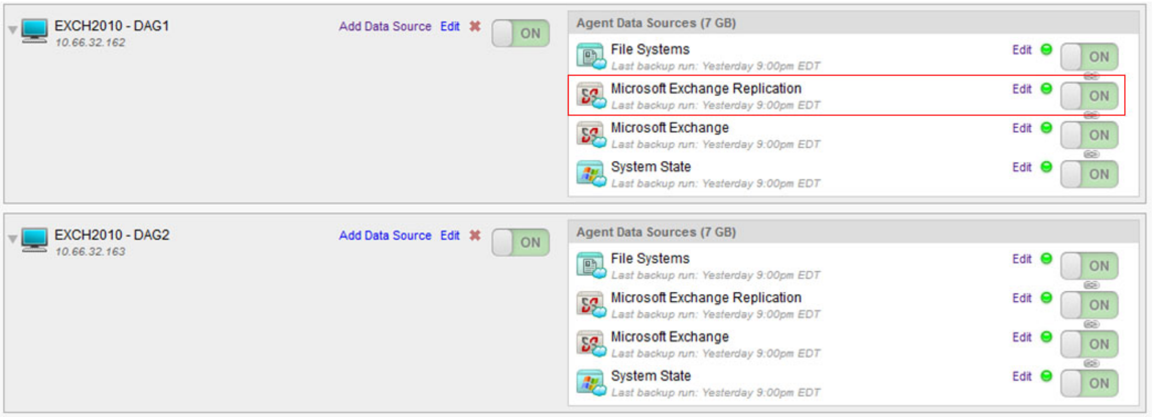

Item Selection

Use *Select All Items* to back up all data recognized by the Barracuda Backup Agent. Use *Select Specific Items* to narrow the scope of your backup.
be purged after 24 hours.

○ Select All Items
● Select Specific Items

Items
⊕ ☑ File Systems
⊕ ☑ Microsoft Exchange
⊖ ☑ Microsoft Exchange Replication
⊕ ☑ Mailbox Database 2080754184
☑ System State

5. Click **Save**. The Exchange Server passive database is added as a data source. The **Sources** page now displays the **Microsoft Exchange Replication** item as a data source to be backed up:


EXCH2010 - DAG1
10.66.32.162

Agent Data Sources (7 GB)

File Systems
Last backup run: Yesterday 9:00pm EDT
Microsoft Exchange Replication
Last backup run: Yesterday 9:00pm EDT
Microsoft Exchange
Last backup run: Yesterday 9:00pm EDT
System State
Last backup run: Yesterday 9:00pm EDT

EXCH2010 - DAG2
10.66.32.163

Agent Data Sources (7 GB)

File Systems
Last backup run: Yesterday 9:00pm EDT
Microsoft Exchange Replication
Last backup run: Yesterday 9:00pm EDT
Microsoft Exchange
Last backup run: Yesterday 9:00pm EDT
System State
Last backup run: Yesterday 9:00pm EDT

How to Back Up Microsoft Exchange Server 2013

This article refers to Barracuda Backup firmware 5.3 and higher, and Microsoft® Exchange Server 2013.

In this article:

- Install the Barracuda Backup Agent
- Set Up the Exchange 2013 Server

Related Articles

- How to Set Up Exchange 2013 Message-Level Backup

Install the Barracuda Backup Agent

Use the following steps to install the Barracuda Backup Agent (Windows) on the Exchange Server 2013:

1. Log in to Barracuda Backup, and select the associated Barracuda Backup Server in the left pane.
2. Go to the **SYSTEM > Software Downloads** page.
3. Download and install the Barracuda Backup Agent (Windows) on the Exchange Server 2013; you do not need to reboot.

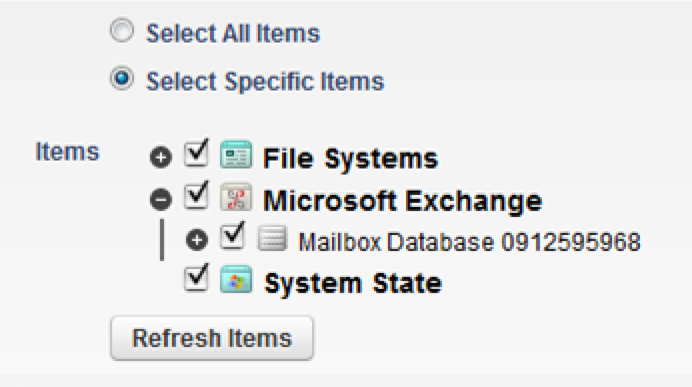
Set Up the Exchange 2013 Server

Use the following steps to set up an Exchange Server 2013 DAG backup on the Barracuda Backup Server:

1. Log in to Barracuda Backup, and select the associated Barracuda Backup Server in the left pane.
2. Go to the **BACKUP > Sources** page, and click **Add Computer**.
3. Add the Exchange Server with the proper hostname or IP address and description.
4. Select **Microsoft Windows** as the **Computer Type**, and click **Save**.
5. In the **Add Data Source** page, select **Barracuda Agent Software** as the **Data Type**, and click **Test Software Connectivity** to verify the

Barracuda Backup Server can communicate with the installed Agent.

6. In the **Item Selection** section, choose to back up all items or specified items (Exchange Databases):

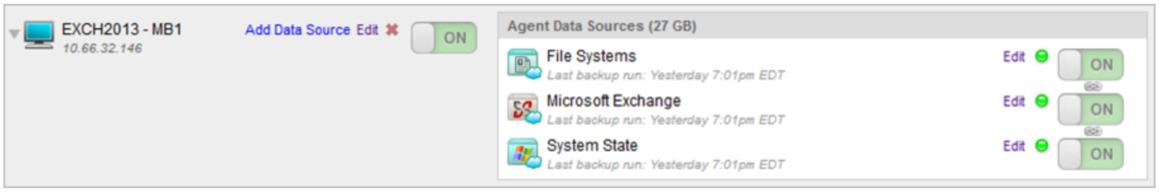


○ Select All Items

● Select Specific Items

Items
- ☑ File Systems
- ☑ Microsoft Exchange
  - ☑ Mailbox Database 0912595968
- ☑ System State

7. Click **Save**. The Exchange Server is added as a data source:



EXCH2013 - MB1
10.66.32.146

Agent Data Sources (27 GB)

File Systems Last backup run: Yesterday 7:01pm EDT	Edit	ON
Microsoft Exchange Last backup run: Yesterday 7:01pm EDT	Edit	ON
System State Last backup run: Yesterday 7:01pm EDT	Edit	ON

How to Set Up Microsoft Exchange Server 2013 Message-Level Backup

This article refers to firmware version 5.3 and higher, and Microsoft® Exchange Server 2013.

In this article:

- Create an Account On the Exchange Server
- Assign Impersonation Rights to the Account
- Add the Exchange Server to Barracuda Backup

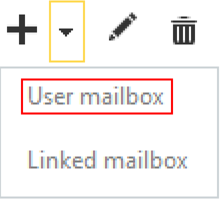
Message-Level Backup
Message-level backup provides a quick way to restore single email messages to the original location or to an alternate mailbox. Message-level backup is not intended to be a disaster recovery option for your Microsoft Exchange environment. The Barracuda Backup Agent allows you to back up the entire Exchange Information Store and should be used for disaster protection.

Create an Account On the Exchange Server

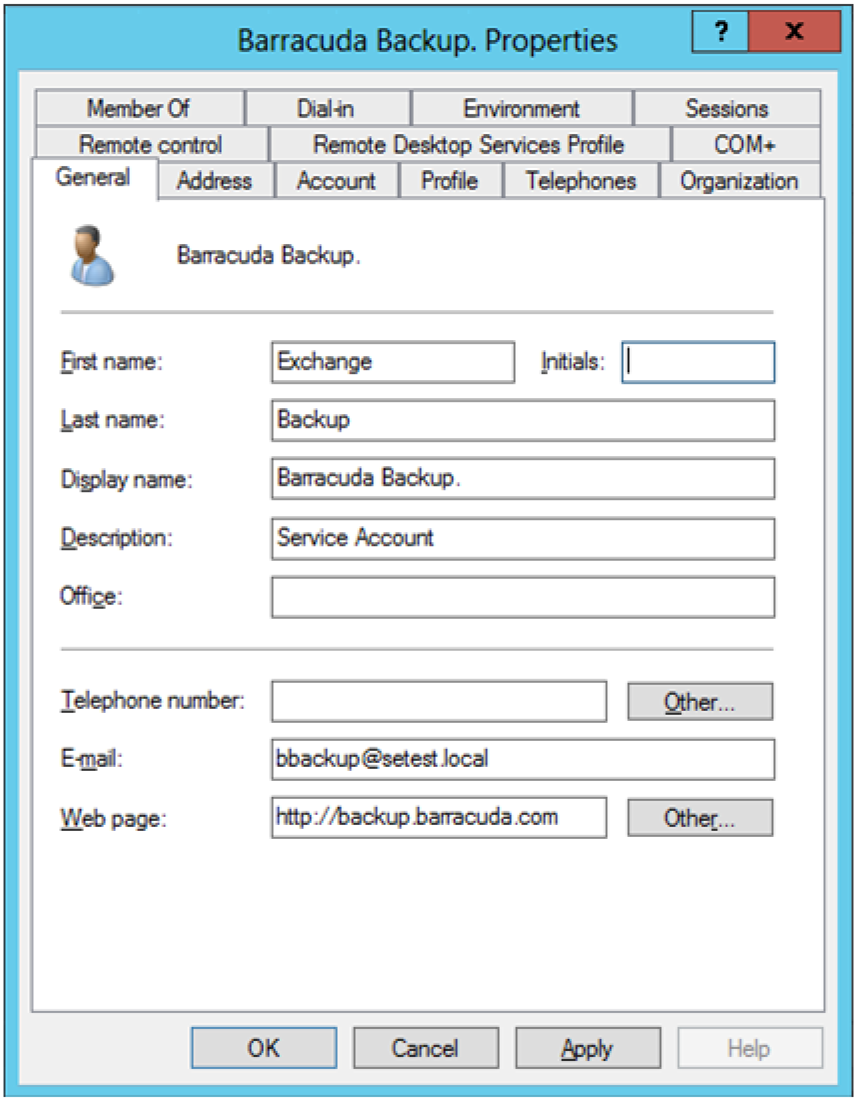
Use the following steps to create an account to be used by Barracuda Backup:

Barracuda Networks recommends using a service-type account rather than an administrator account.

1. Log in to the Exchange Server, click the down arrow next to the plus (**+**) symbol, and click **User mailbox** to create an account to be used by Barracuda Backup to access the emails in each mailbox:


User mailbox
Linked mailbox

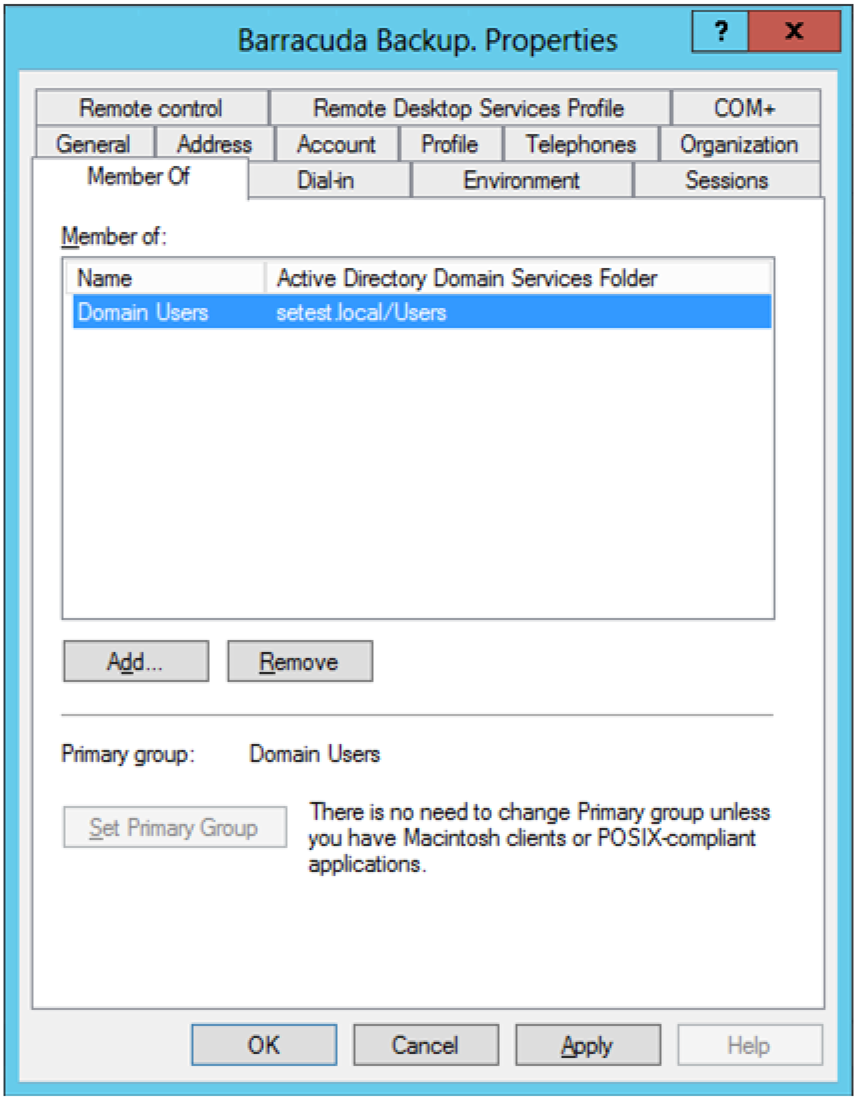
2. In the **new user mailbox** window, enter the new user details, and click **Save**.
3. Double-click the new user mailbox to open the **Properties**:


Barracuda Backup. Properties
?
X
Member Of
Dial-in
Environment
Sessions
Remote control
Remote Desktop Services Profile
COM+
General
Address
Account
Profile
Telephones
Organization
Other...
Other...
OK
Cancel
Apply
Help

Barracuda Backup.

First name: Exchange
Initials:
Last name: Backup
Display name: Barracuda Backup.
Description: Service Account
Office:
Telephone number:
E-mail: bbackup@setest.local
Web page: http://backup.barracuda.com

4. Click the **Member Of** tab, and add the user as a member of the **Domain Users** group; *this is required:*


Barracuda Backup. Properties
?
Remote control
Remote Desktop Services Profile
COM+
General
Address
Account
Profile
Telephones
Organization
Member Of
Dial-in
Environment
Sessions
Add...
Remove
Set Primary Group
OK
Cancel
Apply
Help

Member of:

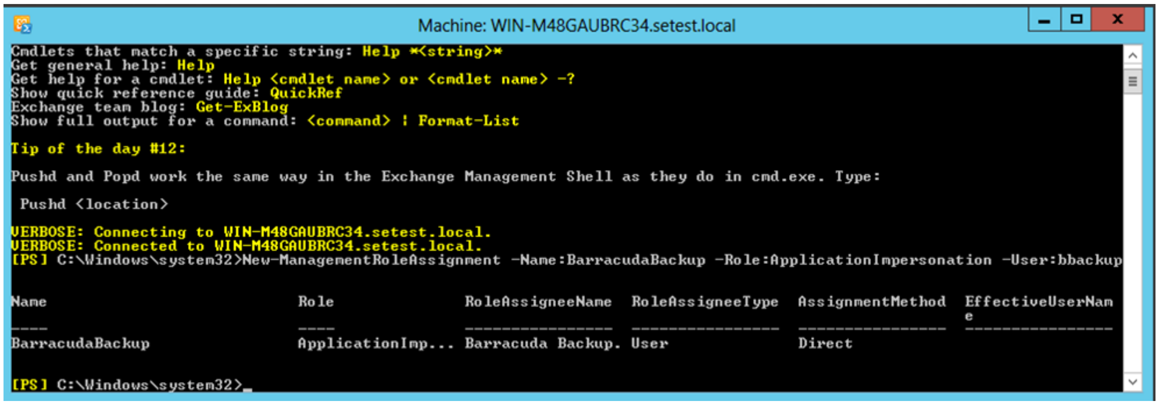
Name	Active Directory Domain Services Folder
Domain Users	setest.local/Users

Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

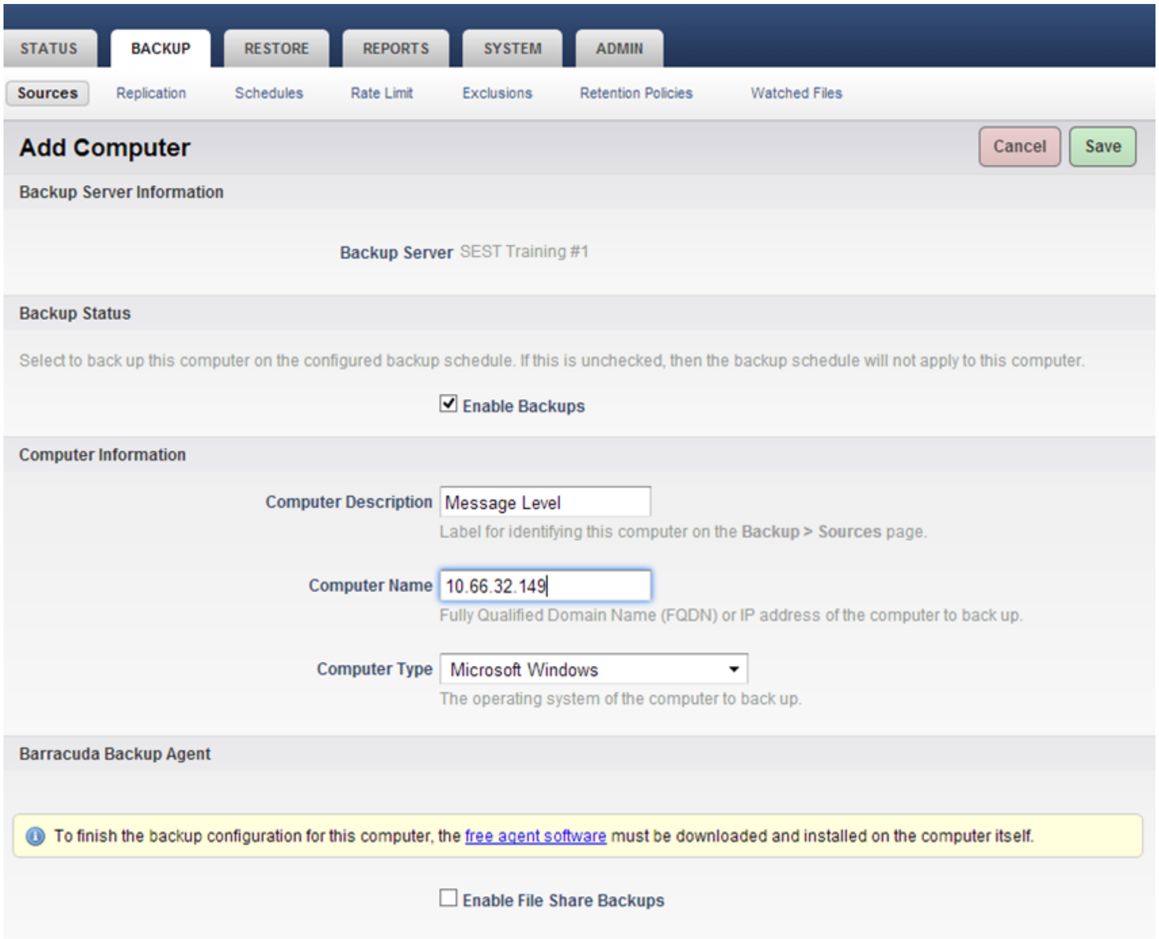
Assign Impersonation Rights to the Account

To assign the account impersonation rights for Exchange:

1. Open the Exchange Management Shell and run the following command, replacing `<ServiceAccount>` with the Service Account username created in the previous section:
   ```
   New-ManagementRoleAssignment -Name:BarracudaBackup
   -Role:ApplicationImpersonation -User: <ServiceAccount>
   ```
   
   Machine: WIN-M48GAUBRC34.setest.local
   ```
   Cmdlets that match a specific string: Help *<string>*
   Get general help: Help
   Get help for a cmdlet: Help <cmdlet name> or <cmdlet name> -?
   Show quick reference guide: QuickRef
   Exchange team blog: Get-ExBlog
   Show full output for a command: <command> | Format-List

   Tip of the day #12:

   Pushd and Popd work the same way in the Exchange Management Shell as they do in cmd.exe. Type:

    Pushd <location>

   VERBOSE: Connecting to WIN-M48GAUBRC34.setest.local.
   VERBOSE: Connected to WIN-M48GAUBRC34.setest.local.
   [PS] C:\Windows\system32>New-ManagementRoleAssignment -Name:BarracudaBackup -Role:ApplicationImpersonation -User:bbackup


   Name                           Role              RoleAssigneeName RoleAssigneeType AssignmentMethod EffectiveUserNam
                                                                                                        e
   ----                           ----              ---------------- ---------------- ---------------- ----------------
   BarracudaBackup                ApplicationImp... Barracuda Backup. User             Direct


   [PS] C:\Windows\system32>_
   ```
2. *Optional*. It is good practice to perform a group policy update on the Exchange Server to replicate permissions. Run the following command either using PowerShell or at a command line:
   ```
   gpupdate /force
   ```

Add the Exchange Server to Barracuda Backup

1. Log in to the Barracuda Backup web interface, go to the **BACKUP > Sources** page, and click **Add Computer**.
2. Enter the Exchange Server details:
    a. **Computer Description -** Enter a label to identify the system.
    b. **Computer Name** - Enter the Exchange Server IP Address or FQDN.
    c. From the **Computer Type** drop-down menu, select **Microsoft Windows**.
    d. Specify whether to enable file share backup:


STATUS
BACKUP
RESTORE
REPORTS
SYSTEM
ADMIN
Sources
Replication
Schedules
Rate Limit
Exclusions
Retention Policies
Watched Files
Cancel
Save

Add Computer

Backup Server Information

Backup Server SEST Training #1

Backup Status

Select to back up this computer on the configured backup schedule. If this is unchecked, then the backup schedule will not apply to this computer.

☑ **Enable Backups**

Computer Information

Computer Description Message Level
Label for identifying this computer on the **Backup > Sources** page.

Computer Name 10.66.32.149
Fully Qualified Domain Name (FQDN) or IP address of the computer to back up.

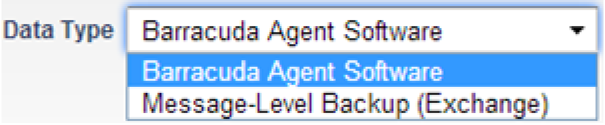
Computer Type Microsoft Windows
The operating system of the computer to back up.

Barracuda Backup Agent

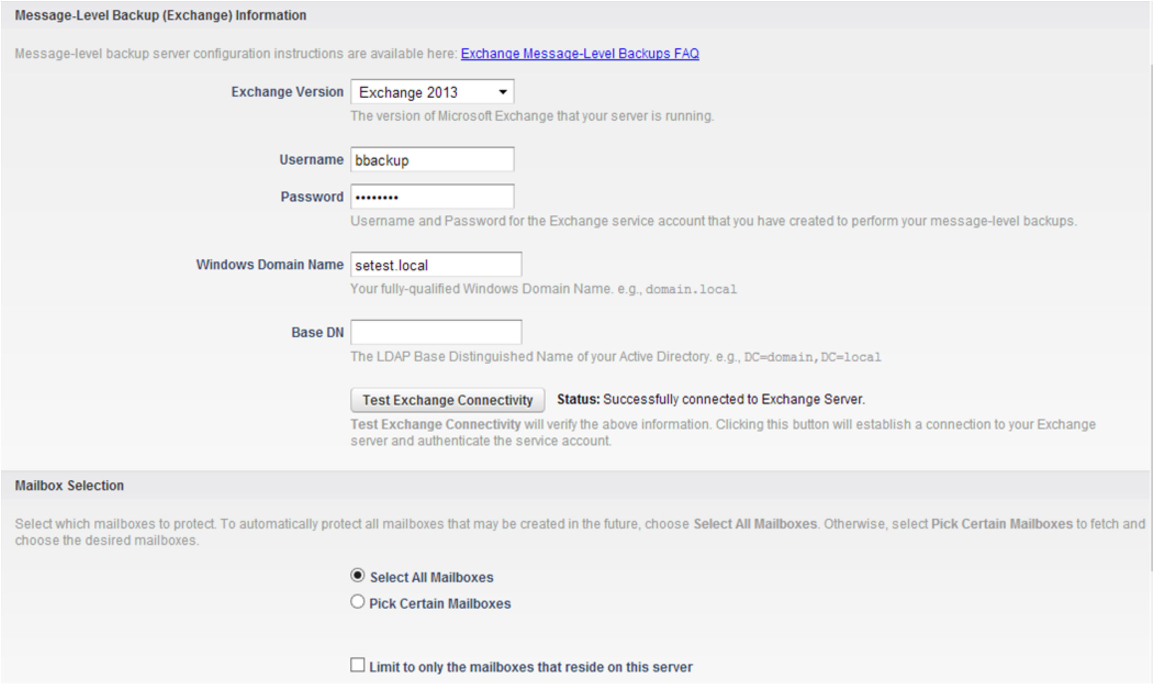
To finish the backup configuration for this computer, the free agent software must be downloaded and installed on the computer itself.

☐ **Enable File Share Backups**

3. Click **Save**. The **Add Data Source** page displays.
4. From the **Data Type** drop-down menu, select **Message-Level Backup (Exchange)**:


Data Type
Barracuda Agent Software
Barracuda Agent Software
Message-Level Backup (Exchange)

5. In the **Message-Level Backup (Exchange) Information** section, enter the following details:
    a. From the **Exchange Version** drop-down menu, select **Exchange 2013**.
    b. In the **Username** and **Password** fields, enter the user login details for the user created in the section Creating an Account On the Exchange Server.
    c. Enter the **Windows Domain Name**.
6. Click **Test Exchange Connectivity** to verify you can connect to the Exchange Server using the entered details.
7. In the **Mailbox Selection** section, select **Select All Mailboxes**:



Message-Level Backup (Exchange) Information

Message-level backup server configuration instructions are available here: Exchange Message-Level Backups FAQ

Exchange Version: Exchange 2013
The version of Microsoft Exchange that your server is running.

Username: bbackup

Password: ••••••••
Username and Password for the Exchange service account that you have created to perform your message-level backups.

Windows Domain Name: setest.local
Your fully-qualified Windows Domain Name. e.g., `domain.local`

Base DN:
The LDAP Base Distinguished Name of your Active Directory. e.g., `DC=domain,DC=local`

Status: Successfully connected to Exchange Server.

Test Exchange Connectivity will verify the above information. Clicking this button will establish a connection to your Exchange server and authenticate the service account.

Mailbox Selection

Select which mailboxes to protect. To automatically protect all mailboxes that may be created in the future, choose **Select All Mailboxes**. Otherwise, select **Pick Certain Mailboxes** to fetch and choose the desired mailboxes.

● Select All Mailboxes
○ Pick Certain Mailboxes

☐ Limit to only the mailboxes that reside on this server

8. Click **Save**.

Microsoft Hyper-V

In this Section

- How to Set Up Microsoft Hyper-V Virtual Machine Backups
- How to Set Up Hyper-V 2008 Clustering
- How to Exclude Individual Virtual Machines from a Hyper-V 2008 Cluster Backup

How to Set Up Microsoft Hyper-V Virtual Machine Backups

> This article refers to Barracuda Backup Server firmware version 5.0 and higher, and Microsoft® Hyper-V 2008, 2008 R2, 2012, and 2012 R2.

In this article:

- Install the Barracuda Backup Agent
- Run the Barracuda Backup Agent as a Service
- Set Up Child Partition Snapshot
- Add the Hyper-V Server
- Set Up Data Sources

Related Articles

- How to Set Up Hyper-V 2008 Clustering
- How to Exclude VMs from a Hyper-V 2008 Cluster Backup
- How to Restore a Microsoft Hyper-V Virtual Machine

The Barracuda Backup Agent provides application-aware backups for Microsoft Hyper-V hypervisor-based virtualization systems and provides support for open file backups, file attributes, and permissions, as well as automatic data source detection.

> ⚠ **Hyper-V 2012 Management Console**
> Hyper-V 2012 Management Console tasks are disabled during backups.

Install the Barracuda Backup Agent

Use the following steps to install the Barracuda Backup Agent (Windows) on the Hyper-V Server.

1. Log into the Barracuda Backup web interface.

2. On the **SYSTEM > Software Downloads** page, download **Barracuda Backup Agent (Windows)** to each Hyper-V Server you want to back up.
3. On the Hyper-V Server, double-click the Agent program to launch the installer.
4. In the Installation Manager, click the **Install** icon.
5. Click **Next** to install the software in the installation directory.
6. When installation is complete, click **OK** to close the window.

Run the Barracuda Backup Agent as a Service

Once installed, complete the following to run the service:

1. On the Hyper-V server, click **Start > Run**, and type:`services.msc`
2. Press **Enter** to run the service**.**

Set Up Child Partition Snapshot

In the Hyper-V console, navigate to the **Settings** on each virtual machines, and under **Integrations settings**, select **Backup (Volume Snapshot)**; if you do not turn on this option, the default backup is set to **Saved State** which can cause issues during restoration.

> ⓘ A *Child Partition Snapshot* backs up the virtual machine by building an **.avhd** snapshot file by using the guests operating system (the virtual machine) VSS writers to read the files internally without having to pause the system. Conversely, a *Saved State* backup uses the host system (physical machine) VSS writers *only* and pauses the guest system to build a backup.

The Saved State backup is *not recommended* as it temporarily stops the virtual machine to back it up, which can cause issues when restoring virtual SQL or Exchange environments from such a backup.

Add the Hyper-V Server

Use the following steps to add Hyper-V Server data sources.

1. Once the agent is installed, select the Barracuda Backup Server in the left pane, and on the **BACKUP > Sources** page, click **Add Computer**.
2. Enter the following details for the Hyper-V Server:
    - **Enable Backups** - Turn on to back up the Hyper-V Server based on the configured backup schedule, or turn off if the backup schedule does not apply.
    - **Computer Description** - Enter a name to identify the server on the **BACKUP > Sources** page.
    - **Computer Name** - Enter the fully qualified domain name (FQDN) or IP address of the Hyper-V Server.
    - **Computer Type** - Select **Microsoft Windows** from the drop-down menu.
3. Click **Save**. The **Add Data Source** page displays.

Set Up Data Sources

In the **BACKUP > Sources > Add Data Source** page, enter the following details:

1. Select **Barracuda Agent Software** from the **Data Type** drop-down menu.
2. The **Backup Status** section displays based on your selection when setting up the server.
3. Click **Test Software Connectivity** to verify the Barracuda Backup Server can communicate with the Barracuda Backup Agent (Windows).
    - If the test is *not* successful, click **Cancel** and verify the following:
        - The FQDN or IP address was entered correctly.
        - The Barracuda Backup Agent (Windows) is installed and running on the server.
    - If the test returns successful, continue to step 4.
4. In the **Item Selection** section, select whether to **Select All Items** or click **Select Specific Items** to select individual files and folders for backup.
5. If you are backing up to Barracuda Cloud Storage, turn on **Replicate to Barracuda Cloud Storage**.
6. If you want to replicate data to another Barracuda Backup Server, turn on **Replicate to Other Barracuda Backup Servers**, and click **Add a new Backup Server**.
7. In the **Add Destination** page, enter the details for the Barracuda Backup Server to which you wish to replicate, and click **Save**.

How to Set Up Hyper-V 2008 Clustering

> This article refers to Barracuda Backup firmware version 5.3 and higher, and Microsoft ® Hyper-V 2008 and 2008 R2 hypervisor-based virtualization systems. This article assumes Hyper-V is installed and configured.

In this article:

- Install the Barracuda Backup Agent
- Run the Barracuda Backup Agent as a Service
- Set Up Child Partition Snapshot
- Add the Hyper-V Server

Related Articles

- How to Restore a Microsoft Hyper-V Virtual Machine
- How to Set Up Microsoft Hyper-V Virtual Machine Backups
- How to Exclude Individual Virtual Machines from a Hyper-V 2008 Cluster Backup

The Barracuda Backup Agent provides application-aware backups for Microsoft Hyper-V hypervisor-based virtualization systems and provides support for open file backups, file attributes, and permissions, as well as automatic data source detection.

> ⚠ **CSV Utilization**
> Because of the Microsoft feature Redirected access, in cases where cluster shared volumes (CSVs) are being utilized, you must stagger backup schedules, or schedule backups for each source/host at separate times. For more information, refer to the Microsoft TechNet article Event ID 5136 - Cluster Shared Volume Functionality.

Install the Barracuda Backup Agent

Use the following steps to install the Barracuda Backup Agent on the Hyper-V Server.

1. Log in to the Barracuda Backup web interface, and select the associated Barracuda Backup Server in the left pane.
2. On the **SYSTEM > Software Downloads** page, download **Barracuda Backup Agent (Windows)** to each Hyper-V Server you to want to back up.
3. On the Hyper-V Server, double-click the Agent program to launch the installer.
4. In the Installation Manager, click the **Install** icon.
5. Click **Next** to install the software in the installation directory.
6. When installation is complete, click **OK** to close the window.

Run the Barracuda Backup Agent as a Service

Once installed, complete the following to run the service:

1. On the Hyper-V server, click **Start > Run**, and type: `services.msc`
2. Press **Enter** to run the service.

Set Up Child Partition Snapshot

In the Hyper-V console, navigate to the **Settings** on each virtual machines, and under **Integrations settings**, select **Backup (Volume Snapshot)** ; if you do not turn on this option, the default backup is set to **Saved State** which can cause issues during restoration.

> ⓘ A *Child Partition Snapshot* backs up the virtual machine by building an **.avhd** snapshot file by using the guests operating system (the virtual machine) VSS writers to read the files internally without having to pause the system. Conversely, a *Saved State* backup uses the host system (physical machine) VSS writers *only* and pauses the guest system to build a backup.

The Saved State backup is *not recommended* as it temporarily stops the virtual machine to back it up, which can cause issues when restoring virtual SQL or Exchange environments from such a backup.

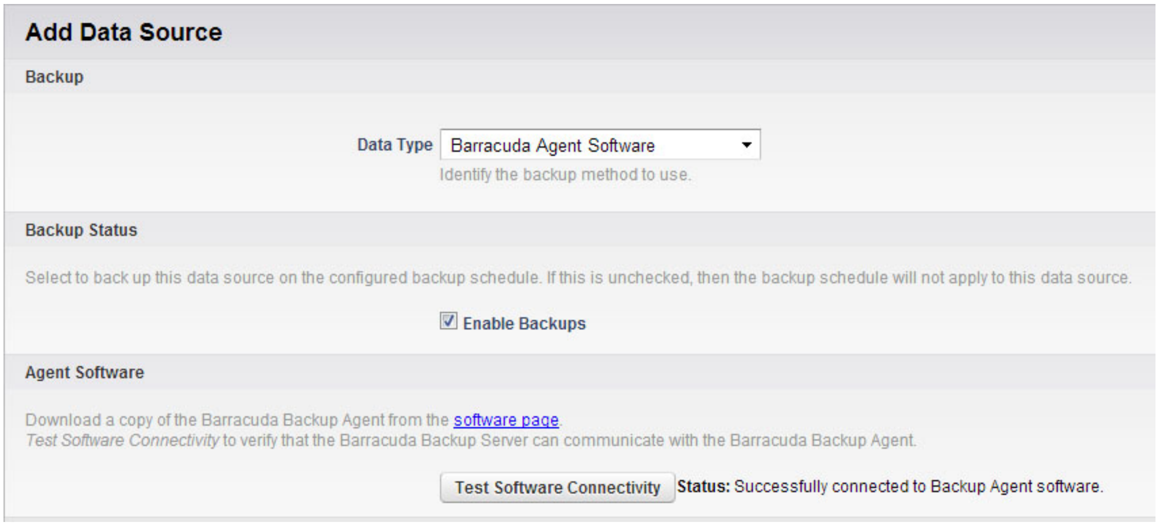
Add the Hyper-V Server

Use the following steps to add Hyper-V Server data sources.

1. Once the agent is installed, select the Barracuda Backup Server in the left pane, and on the **BACKUP > Sources** page, click **Add Computer**.
2. Enter the following details for the Hyper-V Server:
    - **Enable Backups** - Turn on to back up the Hyper-V Server based on the configured backup schedule, or turn off if the backup schedule does not apply.
    - **Computer Description** - Enter a name to identify the server on the **BACKUP > Sources** page.
    - **Computer Name** - Enter the fully qualified domain name (FQDN) or IP address of the Hyper-V Server.

- **Computer Type** - Select **Microsoft Windows** from the drop-down menu.

3. Click **Save**. The **Add Data Source** page displays.
4. Select **Barracuda Agent Software** as the **Data Type**, and click **Test Software Connectivity** to verify connection to the Backup Agent:



Add Data Source

Backup

Data Type: Barracuda Agent Software

Identify the backup method to use.

Backup Status

Select to back up this data source on the configured backup schedule. If this is unchecked, then the backup schedule will not apply to this data source.

☑ Enable Backups

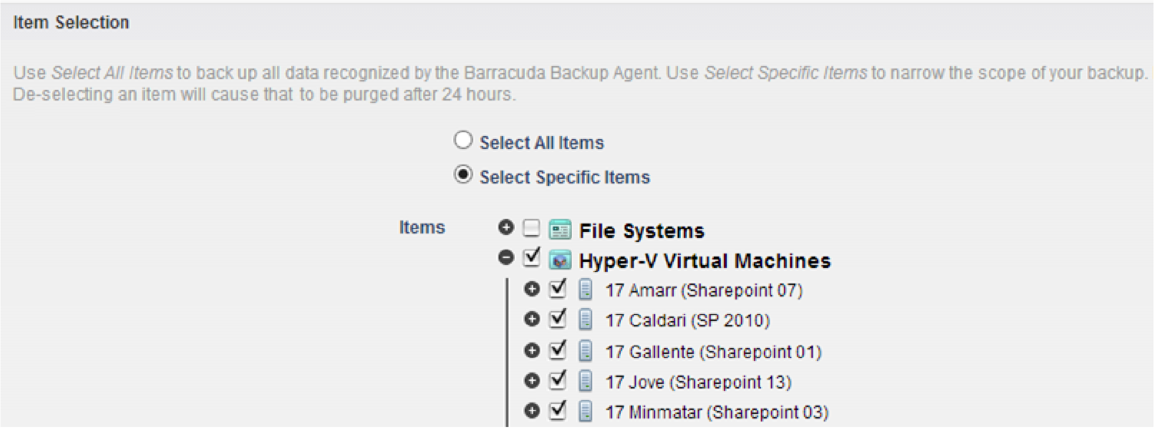
Agent Software

Download a copy of the Barracuda Backup Agent from the software page.

Test Software Connectivity to verify that the Barracuda Backup Server can communicate with the Barracuda Backup Agent.

Status: Successfully connected to Backup Agent software.

5. In the **Item Selection** section, click **Select All Items** to back up all content, or click **Select Specific Items** , and specify the items to be backed up:



Item Selection

Use *Select All Items* to back up all data recognized by the Barracuda Backup Agent. Use *Select Specific Items* to narrow the scope of your backup. De-selecting an item will cause that to be purged after 24 hours.

○ Select All Items

● Select Specific Items

Items

- ☐ File Systems
- ☑ Hyper-V Virtual Machines
  - ☑ 17 Amarr (Sharepoint 07)
  - ☑ 17 Caldari (SP 2010)
  - ☑ 17 Gallente (Sharepoint 01)
  - ☑ 17 Jove (Sharepoint 13)
  - ☑ 17 Minmatar (Sharepoint 03)

Important

In cases where virtual machines have the potential of moving between hosts, *you must:*

- Click **Select All Items** in the **Item Selection** section of the web interface to select the *entire host*.
- Edit the Barracuda Agent **bbconfig.ini** file to exclude certainly virtual machines.

6. Click **Save**.
7. Repeat steps 1 through 6 for each host in the cluster.

This article refers to Barracuda Backup firmware version 5.3 and higher, and Microsoft® Hyper-V 2008 and 2008 R2 hypervisor-based virtualization systems. This article assumes Hyper-V is installed and configured.

Related Articles

- How to Set Up Hyper-V 2008 Clustering
- How to Set Up Microsoft Hyper-V Virtual Machine Backups

In some instances it may be necessary to exclude certain virtual machines from backup when implementing a clustered Hyper-V environment. To do so, you must configure the Barracuda Backup Agent (Windows) to ignore those virtual machines you wish to exclude from backup.

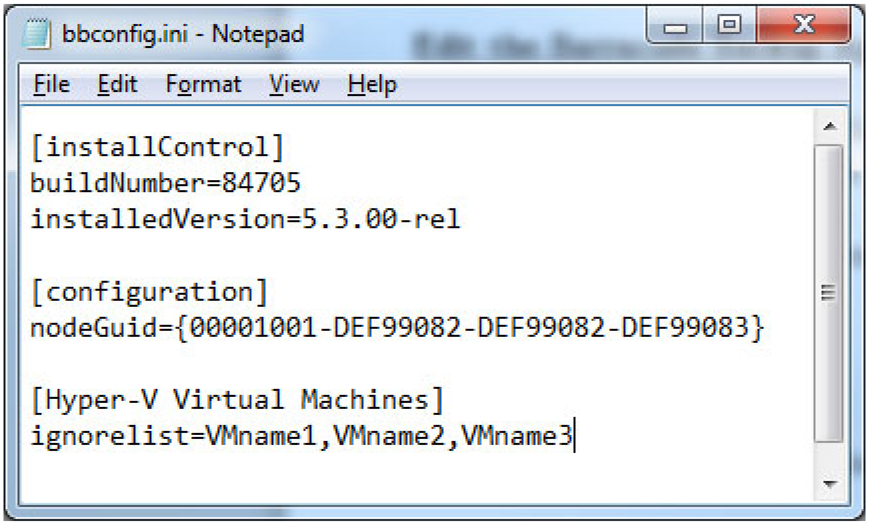
Edit the Barracuda Backup Agent

Use the following instructions to edit the Barracuda Backup Agent on the Hyper-V Server:

1. On the Hyper-V Server where you installed the Barracuda Backup Agent (Windows), open Services.
2. Right-click on the Service **Barracuda Backup Agent**, and click **Stop**. The Service is now stopped.
3. Open the **bbconfig.ini** file in Notepad; the file is located in the following directory: **/Program Files/Barracuda/Barracuda Backup Agent/config/bbconfig.ini**
4. Add the following lines to the end of the file:

   ```
   ignorelist=VMname1,VMname2,VMname3
   ```

   For example:



```
[installControl]
buildNumber=84705
installedVersion=5.3.00-rel

[configuration]
nodeGuid={00001001-DEF99082-DEF99082-DEF99083}

[Hyper-V Virtual Machines]
ignorelist=VMname1,VMname2,VMname3
```

5. Save and close the file.
6. Open Services once again.
7. Right-click on the Service **Barracuda Backup Agent**, and click **Start**. The **Status** field should display as **Started**.

Microsoft SQL Server

In this Section

- How to Back Up Microsoft SQL Server Databases
- How to Enable VSS Backups for Microsoft SQL Server

How to Back Up Microsoft SQL Server Databases

This article refers to Barracuda Backup firmware 5.0 and higher, and Microsoft SQL Server running the Barracuda Backup Agent (Windows).

In this article:

- Add the SQL Server as a Data Source
- Create Backup Schedules

- Modify Your Backup Rate Limit (Optional)
- Exclude Files from a Backup (Optional)
- Create Data Retention Policies
- Check Backup Reports

Related Articles
- Schedules Page - Retention Policies Page - Backing Up a SQL Server Database Using VSS

Add the SQL Server as a Data Source

Use the following steps to configure the SQL Server and data sources using the Barracuda Backup Agent (Windows):

1. Log in to Barracuda Backup, and select the associated Barracuda Backup Server in the left pane.
2. Go to the **SYSTEM > Software Downloads** page.
3. Download and install the Barracuda Backup Agent (Windows) on the SQL Server.
4. Go to the **BACKUP > Sources** page, and click **Add Computer** to identify the system.
5. Enter the details for your SQL Server, and click **Save**.
6. In the **Data Sources** page, select **Barracuda Agent Software** as the **Data Type**, and click **Test Software Connectivity** to verify the Barracuda Backup Server can connect to the Agent installed on the SQL Server.
7. In the **Items Selection** section, click **Select All Items** to backup the entire Server, or click **Select Specific Items** to select individual items for backup.
8. To back up to Barracuda Cloud Storage, turn on **Replicate to Barracuda Cloud Storage**.
9. Click **Save**. The SQL Server is added as a data source.

Create Backup Schedules

> Note that schedules are automatically created (with the default set to back up every day at 8:00PM) when a data source is created *except* if a schedule specifying *all* data sources already exists.

Now that you have configured your computers and data sources, you can create backup schedules, either individually or for all sources. If no schedule is created for a data source then it will not be backed up.

To create a backup schedule:

Click here to expand...

1. Log in to the Barracuda Backup web interface, and select the associated Barracuda Backup Server in the left pane.
2. Go to the **BACKUP > Schedules** page. Click **Add a Schedule** and fill in the information on the **Add Backup Schedule** page:
    - **Schedule Name** - Enter a label to identify the backup schedule.
    - **Items to Back Up** - Turn on **Apply to All Computers and Data Sources for this Barracuda Backup Server** to back up all content, or turn this option off to expand and select individual items for backup.
    - **Schedule Timeline** - Turn on the days on which the back up is to run.
    - **Daily Backup Timeline** - Enter the start time; turn on **Repeat** if you wish to specify a time period and end date to repeat the backup.
3. If the backup schedule is for Microsoft SQL or Microsoft Exchange, you must specify the type of backup to run:
    - **Full** - This backup type performs a full backup of data, including the transaction logs.
    - **Log** - This backup type only backs up transaction logs created since the last full backup.
    - **Smart** - This backup type is a combination of the full backup and the transaction log backup, minimizing the impact of backups on network resources necessary to transfer data off site. Barracuda Networks recommends this backup type for SQL and Exchange servers.
      With the Smart Backup type, threshold values are used to determine when to switch between full and log backups. The minimum threshold value specifies how many days Barracuda Backup continues to back up transaction logs before another full backup is run. After the minimum threshold value is met, Barracuda Backup determines whether to perform another backup based on the binary data queue. If the binary data queue size exceeds 1 GB, Barracuda Backup continues

the transaction log backup until the maximum threshold level is met, or the queue size drops below 1 GB.

Modify Your Backup Rate Limit (Optional)

Rate limits control the data replication rate to Barracuda Cloud Storage or other offsite storage locations. You can limit Internet bandwidth consumption during peak usage times, and schedule backups for non-peak hours.

Your initial offsite backup may take on the order of days to complete but all of the data is backed up locally on the Barracuda Backup Server during this period. After the initial large transfer is complete, replicating your data offsite should complete with only a few hours of transfer each day. By default, Barracuda Backup is configured to run full speed data transfers at night so that bandwidth is not affected while most people are at work. An alternate rate limit allows you to adjust the limit speed and time interval.

The length of transfer time it will take to get your data offsite is impacted by the compression and de-duplication rates on your data, the uplink speed of your Internet connection, the amount of data that changes every day, and any speed limits you apply to Barracuda Backup.

To adjust the backup rate limit:

Click here to expand...

1. Log in to the Barracuda Backup web interface, and select the associated Barracuda Backup Server in the left pane.
2. On the **BACKUP > Rate Limit** page, select a Barracuda Backup Server on the left menu and create or edit the rate limit.
3. You can specify a default rate limit and an alternate rate limit which is maintained only during the specified time periods.

Exclude Files from a Backup (Optional)

You can create exclusion rules that use pattern matching to identify directory or file names that are not to be backed up. Files which are typically excluded from backups include temporary files, music, movies and other files which are not essential for business needs.

Use the following steps to create an exclusion rule:

Click here to expand...

1. Log in to the Barracuda Backup web interface, and select the associated Barracuda Backup Server in the left pane.
2. Go to the **BACKUP > Exclusions** page of the Barracuda Backup web interface. Click **Add an Exclusion**.
3. Fill in the information on the **Add an Exclusion** page:
   a. **Exclusion Rule Name** - Enter a descriptive label to identify the exclusion rule.
   b. **Add Exclusions to Reports** - Turn on to include exclusions in reports, and turn off to exclude the rules from reports.
   c. **Apply Recursively to Sub Directories -** Specify whether to apply the exclusion rule recursively to sub directories.
   d. **Where to Exclude** - Turn **Apply to All Computers and Data Sources for this Barracuda Backup Server** on to apply the exclusion rule to all, or turn off, then expand and select individual items to which to apply the exclusion rule.
4. Specify what to exclude in the **What to Exclude** section:
   a. From the **Preset Expressions** menu, select the content to exclude, for example, **Video files**, then click **Add**.
   b. In the **Expressions** field, enter a search string to exclude, for example, ***.mp3**, then click **Add**.
5. Click **Save** at the top of the page to add the exclusion rule.

To edit an existing exclusion rule, go to the **BACKUP > Exclusions** page of the Barracuda Backup web interface, and click **Edit** following the exclusion rule you wish to edit. Make the desired changes, then click **Save**.

To delete an exclusion rule, go to the **BACKUP > Exclusions** page of the Barracuda Backup web interface, and click the **Delete** icon following the exclusion rule you wish to remove. Click **OK** to confirm you wish to remove the rule.

Create Data Retention Policies

Data is retained based on a traditional grandfather-father-son (daily-weekly-monthly) rotation model. You can specify how long to keep daily, weekly, monthly, and yearly backups by creating data retention policies. Different retention policies can be created for different sets of data including files, data backed up by the Barracuda Backup Agent (Exchange, SQL, System State), and email messages.

You can create one policy for all of the computers and data sources on a Barracuda Backup Server or multiple policies that each include some subset of the data.

To set retention policies:

Click here to expand...

1. Log in to the Barracuda Backup web interface, and select the associated Barracuda Backup Server in the left pane.
2. Go to the **BACKUP > Retention Policies** page, click **Add a Retention Policy**, and enter a name to identify the policy.
3. In the **Items to Retain** section, specify the data sources to which the retention policy applies; the **Retention Timeline** section displays. Select a timeline template on which to base your retention policy, or specify your own revision timeline.

4. Select the desired **Removed Files Rule** setting, and click **Save**.

When data is removed according to a retention policy, it is deleted from both the local Barracuda Backup Server and the offsite storage locations. Removed files that have been backed up using Network File Shares Protocol or SSHFS may be retained for a longer period of time, according to the configuration. Otherwise, once your data has been purged, it is gone forever. Purging applies to historic file revisions only; your current data is not impacted by a retention policy.

Check Backup Reports

View reports on an ongoing basis as needed. The **REPORTS > Backup** page contains detailed backup reports. A list of in progress backups displays at the top of the page, and once a backup is complete, a detailed report displays in a table by device. Click Details following the report you wish to view.

How to Enable VSS Backups for Microsoft SQL Server

This article refers to firmware version 5.3 or higher, and Microsoft® SQL Server® 2012, 2008, 2008 R2, and 2005 SP1 or higher databases.

Related Articles

- How to Back Up Microsoft SQL Server Databases
- Barracuda Backup Agent File Structure

Barracuda Backup protects Microsoft SQL Server 2012 using the Microsoft Volume Shadow Copy Service (VSS). With VSS, Barracuda Backup is able to perform full and differential database backups.

In Barracuda Backup firmware version 5.2 and earlier, the Barracuda Backup Agent utilized the SQL Server Virtual Device Interface (VDI) to implement SQL database backup and restore operations. The VDI technology provides the ability to backup and restore full and incremental backups of the SQL databases and is enabled by default on the Barracuda Backup Agent. In firmware 5.3 and higher, the Barracuda Backup Agent can leverage VSS for other versions of SQL.

Requirements
Verify the following is true on the Microsoft SQL Server:

- Barracuda Backup Agent is installed, and
- The SQL Server has been added as a Barracuda Backup data source.

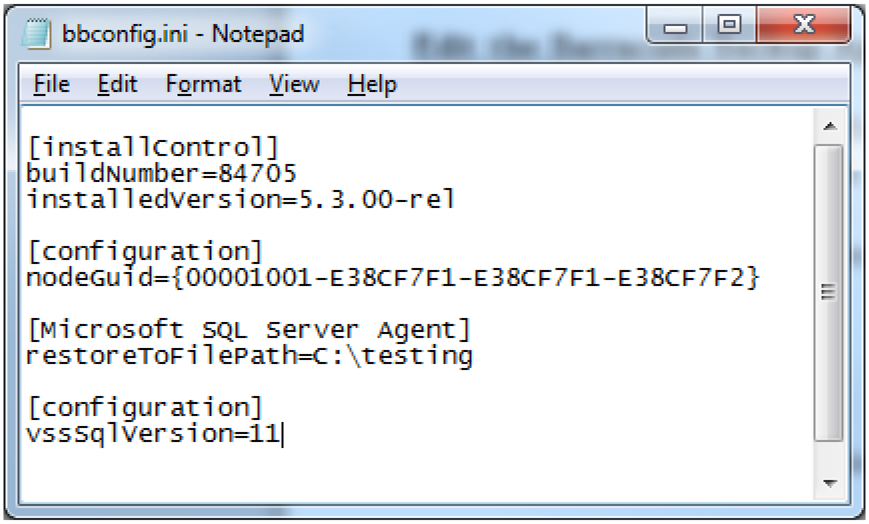
Edit the Barracuda Backup Agent

Use the following instructions to edit the Barracuda Backup Agent installed on the SQL Server:

1. On the SQL Server where the Barracuda Backup Agent is installed, open Services.
2. Right click on the Service **Barracuda Backup Agent**, and click **Stop**. The Service is now stopped.
3. Open the **bbconfig.ini** file in Notepad; the file is located in the following directory: **/Program Files/Barracuda/Barracuda Backup Agent/config/bbconfig.ini**
4. Add the following lines to the end of the file based on the installed version of SQL Server.
    - For SQL Server 2012:

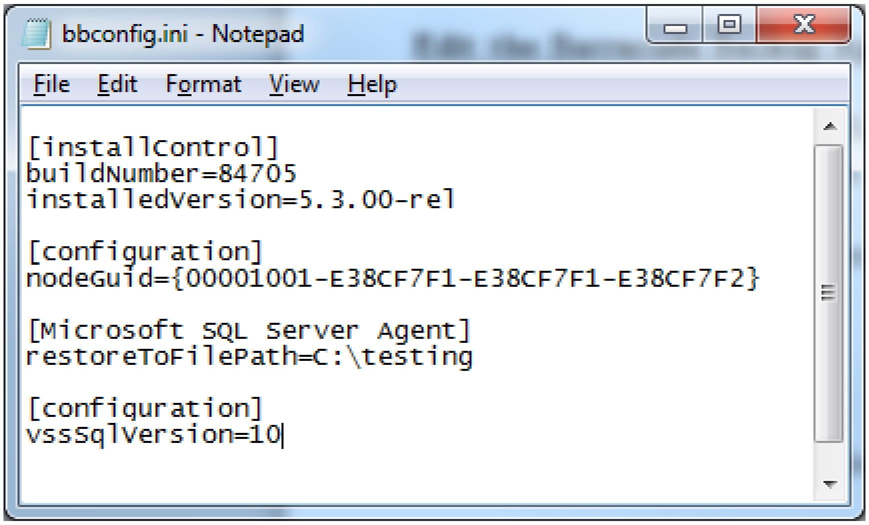
```
[configuration]
vssSqlVersion=11
```

SQL Server Version
In the line `vssSqlVersion=11`, the number **11** represents the major release version of your SQL Server; replace this number accordingly. For example, the major release number for both SQL Server 2008 and SQL Server 2008 R2 is **10**
.


bbconfig.ini - Notepad
File
Edit
Format
View
Help

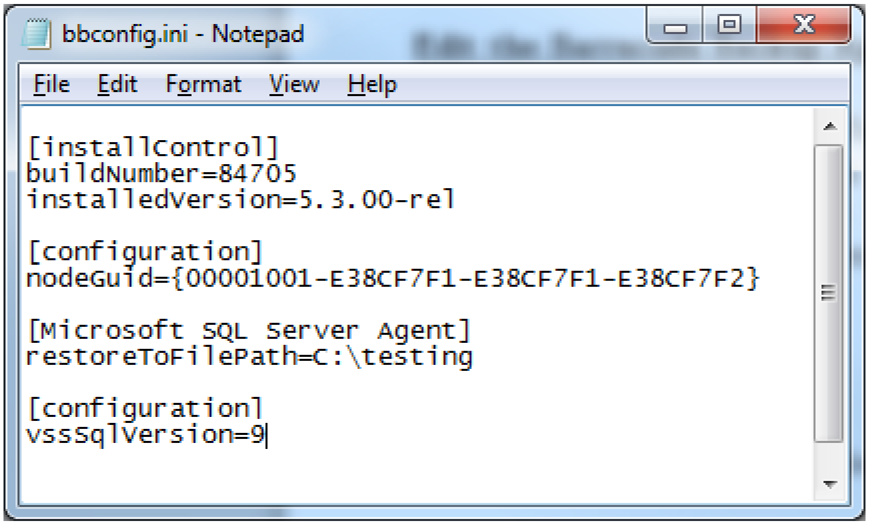
```
[installControl]
buildNumber=84705
installedVersion=5.3.00-rel

[configuration]
nodeGuid={00001001-E38CF7F1-E38CF7F1-E38CF7F2}

[Microsoft SQL Server Agent]
restoreToFilePath=C:\testing

[configuration]
vssSqlVersion=11
```

- For SQL Server 2008 or 2008 R2:
  `[configuration]`
  `vssSqlVersion=10`


bbconfig.ini - Notepad
File
Edit
Format
View
Help

```
[installControl]
buildNumber=84705
installedVersion=5.3.00-rel

[configuration]
nodeGuid={00001001-E38CF7F1-E38CF7F1-E38CF7F2}

[Microsoft SQL Server Agent]
restoreToFilePath=C:\testing

[configuration]
vssSqlVersion=10
```

- For SQL Server 2005 SP1 or higher:
  `[configuration]`
  `vssSqlVersion=9`


bbconfig.ini - Notepad
File
Edit
Format
View
Help

```
[installControl]
buildNumber=84705
installedVersion=5.3.00-rel

[configuration]
nodeGuid={00001001-E38CF7F1-E38CF7F1-E38CF7F2}

[Microsoft SQL Server Agent]
restoreToFilePath=C:\testing

[configuration]
vssSqlVersion=9
```

5. Save and close the file.

6. Open Services once again.
7. Right click on the Service **Barracuda Backup Agent**, and click **Start**. The **Status** field should display as **Started**.

VSS is now enabled to implement full and differential SQL database backup and restore operations.

VMware

In this Section

- How to Set Up a VMware Server and Guests
- VMware Data Recovery Backup and Restore Permissions

How to Set Up a VMware Server and Guests

> This article applies to Barracuda Backup firmware version 4.2 or higher, and VMware® 4.0 and above with the VMware license which includes access to vSphere® Data Recovery API. Note that in Barracuda Backup firmware version 5.4 and higher, you can back up parallel VMware virtual machines (VMs)—up to five VMs per ESX/i host.

In this article:

- Parallel VMware Backup
- Changed Block Tracking
- Configure the Data Source
- Modify the Data Source

Related Articles

- How to Restore a Virtual Machine to its Original Location
- Understanding Changed Block Tracking on Virtual Machines
- VMware Data Recovery Backup and Restore Permissions

Barracuda Backup utilizes the vSphere Data Recovery API to backup and restore the VMware Host configuration as well as VMware guests. VMware host backup provides a comprehensive disaster recovery option for VMs and provides the ability to recover VMs to any VMware host accessible by the Barracuda Backup Server.

> ✓ **Best Practices**
>
> To prevent errors and warnings, and to improve performance when setting up a VMware backup:
>
> - Ensure the datastore has sufficient space;
> - Enable changed block tracking; and
> - Uninstall any third-party backup agents.

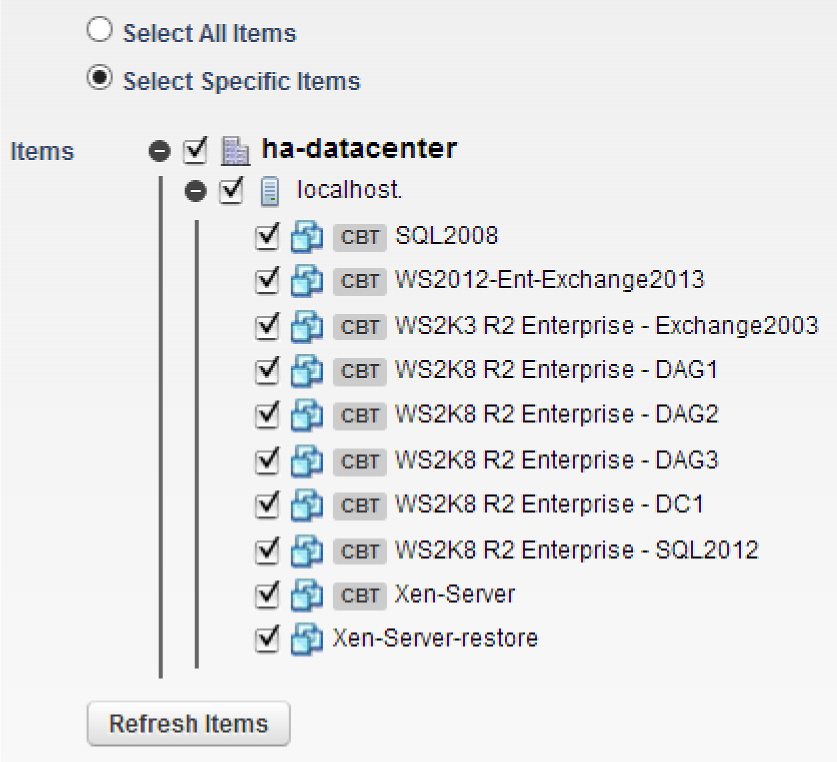
Parallel VMware Backup

In firmware realease 5.3 and higher, you can back up multiple guests on the same host concurrently. The following table lists the default number of guest machines that you can back up simultaneously during a VMware backup by device:

Barracuda Backup Device Number	Default Number of Guest Machines
190	3
390	5
490	7
690	8
890	10
990	15
1090	20

Changed Block Tracking

To avoid warning messages when setting up a VMware backup, you can enable Changed Block Tracking (CBT). When enabled, CBT displays in the data source list:



○ Select All Items

● Select Specific Items

Items
- ☑ ha-datacenter
  - ☑ localhost.
    - ☑ CBT SQL2008
    - ☑ CBT WS2012-Ent-Exchange2013
    - ☑ CBT WS2K3 R2 Enterprise - Exchange2003
    - ☑ CBT WS2K8 R2 Enterprise - DAG1
    - ☑ CBT WS2K8 R2 Enterprise - DAG2
    - ☑ CBT WS2K8 R2 Enterprise - DAG3
    - ☑ CBT WS2K8 R2 Enterprise - DC1
    - ☑ CBT WS2K8 R2 Enterprise - SQL2012
    - ☑ CBT Xen-Server
    - ☑ Xen-Server-restore

Configure the Data Source

Use the following steps to add a computer and configure the data source through Barracuda Backup:

1. Log in to Barracuda Backup as the administrator, and go to the **BACKUPS > Sources** page.
2. Click **Add Computer**, and complete the details for the data source:
   - **Enable Backups** - Turn on to enable backups for the VMware host; this option is turned on by default
   - **Computer Description** - Enter a name to identify the host (for example, ESX, ESXi, vCenter) field
   - **Computer Name** - Enter the name or IP address of the VMware host on the network
   - **Computer Type** - Select **VMware** from the drop-down menu
   - **Username/Password** - Enter the credentials to access the VMware host
3. Click **Test Credentials** to verify the Barracuda Backup Server can communicate with the VMware host.
4. Click **Save** to save the configuration for the new data source; the VMware host data source is detected and added automatically.
5. In the **Add Data Source** page, select the virtual machines you wish to backup:
   - Click **Select All Items** to back up all data recognized by the VMware host, *or*
   - Click **Select Specific Items** and expand the tree to view the virtual machines available for backup on the VMware host; turn on those virtual machines you wish to back up
6. Click **Save** to save the configuration for the data source.

The VMware data source displays in the **Data Sources** page.

Modify the Data Source

Use the following steps to modify the VMware data source:

1. Log in to Barracuda Backup web interface, and select the associated Barracuda Backup Server in the left pane.
2. Go to the **BACKUP > Sources** page.
3. To the right of the VMware data source name, click **Edit**.
4. Make the desired changes, and click **Save**.

This article refers to Barracuda Backup firmware version 5.0 or higher, and VMware® ESX/ESXi host machines, or vCenter Server version 4.0 or higher with vSphere except where noted.

In this article:

- ESX/ESXi Host Machine Permissions
- vCenter Server Role for Backup and Recovery
- vCenter Server Role for Scheduled Backup Operations Permissions
- Barracuda Backup Set Up and Restore Permissions

Related Articles

- VMware Data Recovery Licenses

Additional Resources

- VMware Data Recovery Administration Guide

ESX/ESXi Host Machine Permissions

At a minimum, you must have the following permissions assigned to the user role on an ESX/ESXi virtual machine:

Table 1. ESX/ESXi User Role Permissions.

System	Configuration	Disk Change Tracking
Virtual Machine	Provisioning	Allow read-only disk access Allow virtual machine download
Virtual Machine	State	Create snapshot Remove snapshot
Global		DisableMethods EnableMethods License

If you are using SCSI hot-adding on an ESX/ESXi virtual machine, the user role must have the following permissions:

- All of the permissions listed in Table 1, *and*
- The Barracuda Backup must have all of the permissions listed in Table 2:

Table 2. Barracuda Backup Minimum Permissions.

System	Configuration	Permissions
Datastore		Allocate space
Virtual Machine	Configuration	Add existing disk
		Add new disk
		Add or remove device
		Change resource
		Remove disk
		Settings

vCenter Server Role for Backup and Recovery

If you wish to assign privileges to a vCenter Server user or a user in Active Directory (AD), you can create a new user with the VMware vCenter roles.

The recovery operation requires privileges for operations on hosts, networks, and datastores. You must apply this new role to the Datacenter object or higher in the VMware vCenter Server hierarchy for the user specified in the **VMcuser** option and **Propagate to Child Object** must be turned on when adding the permission.

To create a vCenter Server role for backup and recovery operations, log in to the vCenter Server using the vSphere Client, and add the permissions listed in Table 3:

Table 3. vCenter Server Role Permissions.

Location	Configuration	Permissions
Datastore		• Allocate space • Browse datastore • Low-level file operations
Global		• Licenses
Guest Operations(1)(2)		• Guest Operation Modifications • Guest Operation Program Execution • Guest Operation Queries
Network		• Assign network
Resource		Assign virtual machine to
vApp		• Add virtual machine • Assign resource pool • Create
Virtual Machine	Configuration	• Add existing/new disk • Add/remove device • Advanced • Change CPU count • Change resource • Disk change tracking • Disk Lease • Host USB device • Memory • Modify device setting • Raw device • Reload from path(4) • Remove disk • Rename • Reset guest information • Settings • Swapfile placement • Upgrade virtual hardware
Virtual Machine	Inventory	• Create new • Register • Remove • Unregister
Virtual Machine	Provisioning	• Allow disk access • Allow read-only disk access • Allow virtual machine download
Virtual Machine(2)	Snapshot Management(2) > State(2)	• Create snapshot • Remove snapshot • Revert to snapshot

Virtual Machine(3)	State(3)	- Create snapshot - Remove snapshot - Revert to snapshot
Notes: (1) Guest Operations permissions are necessary *only* if you are using Data Protection for VMware to protect Microsoft Exchange Server or Microsoft SQL Server applications running inside a virtual machine guest. (2) vSphere 5.0 only. (3) vSphere 4.0 only. (4) vCenter Server 4.1 only.		

vCenter Server Role for Scheduled Backup Operations Permissions

To add a vCenter Server role for backup operations only, add a role using the vSphere Client, and add the permissions listed in Table 4.

ⓘ You must apply this new role to the target host (ESX/ESXi) object or higher in the VMware vCenter Server hierarchy for the user specified in the **VMcuser** option, and **Propagate to Child Object** must be turned on when adding the permission.

Table 4. vCenter Server Role for Backup Operations Permissions.

Location	Configuration	Permissions
Guest Operations(1)(2)		- Guest Operation Modifications - Guest Operation Program Execution - Guest Operation Queries
Virtual Machine	Configuration	- Disk change tracking - Disk Lease
Virtual Machine	Provisioning	- Allow read-only disk access - Allow virtual machine download
Virtual Machine(2)	Snapshot Management(2) > State(2)	- Create snapshot - Remove snapshot
Virtual Machine(3)	State(3)	- Create snapshot - Remove snapshot
Notes: (1) Guest Operations permissions are necessary *only* if you are using Data Protection for VMware to protect Microsoft Exchange Server or Microsoft SQL Server applications running inside a virtual machine guest. (2) vSphere 5.0 only. (3) vSphere 4.0 only.		

Barracuda Backup Set Up and Restore Permissions

To set up and restore a VMware virtual machine as a data source in the Barracuda Backup web interface, you must have administrator privileges to the virtual machine. Once your credentials are verified and the data source is set up and backups are enabled, use the **RESTORE** page to restore a virtual machine. For more information on this VMware requirement, refer to the VMware Data Recovery Administration Guide available on the VMware website.

How to Back Up Microsoft Active Directory

This article refers to Barracuda Backup firmware version 5.0 or higher, and Microsoft® Active Directory (AD).

Barracuda Networks recommends enabling Active Directory Recycle Bin before backing up content. Refer to the Microsoft TechNet article Enable Active Directory Recycle Bin for details.

Backing up the AD is done on one or more Active Directory Domain

Controllers, and is performed by backing up the System State on those servers. Barracuda Backup utilizes the Barracuda Backup Agent (Windows) to back up and restore the Microsoft Windows System State. Back up the System State to have a backup of critical system-related components.

The System State backup contains the following:

- Local Registry
- COM+ Class Registration Database
- System Boot Files
- Active Directory Database File (NTDS.DIT) for Domain Controllers
- SYSVOL folder

Related Articles

- Restore a Windows Server 2012 AD Object from the AD Recycle Bin
- Enable AD Recycle Bin on Windows Server 2012
- Restore a Windows Server 2008 R2 AD Object from the AD Recycle Bin
- Enable AD Recycle Bin on Windows Server 2008 R2

A System State backup allows you to recover to a known "good" system state after a hardware or software crash.

Use the following steps to add a computer and configure the data source on Barracuda Backup:

1. Log in to the Barracuda Backup web interface, and select the associated Barracuda Backup Server in the left pane.
2. Go to the **BACKUP > Sources** page, and click **Add Computer** to identify the system.
3. Enter the data description, and select the appropriate data type; click **Save**.
4. The **Add Data Source** page displays. Choose to select all items or specified items.

   System State must be selected to restore AD.

5. Turn on **Replicate to Other Barracuda Backup Servers**, and click **Save.**
6. Once configured, create a schedule to define how often the data is to be backed up on the **BACKUP > Schedules** page, and define a policy for how long the data is to be retained on the **BACKUP > Retention Policies** page.

Tombstone Lifetime
To ensure a good backup you should be aware of the tombstone lifetime. The tombstone lifetime is the number of days before a deleted object is removed from the directory services. A backup that is older than the tombstone lifetime (the default is 60 days) set in Active Directory is not a good backup. At a minimum, perform at least two backups within the tombstone lifetime. Active Directory incorporates the tombstone lifetime into the backup and restore process as a means of protecting itself from inconsistent data.

How to Back Up and Restore a Microsoft SharePoint SQL Database

This article refers to Barracuda Backup firmware version 5.0 and higher, and Microsoft® SharePoint® 2003, 2007, and 2010.

In this article:

- Install the Barracuda Backup Agent
- Add SharePoint as a Data Source
- SharePoint Backup Considerations
- Site Recycle Bin
- SharePoint Backup Best Practices
- Backing Up SharePoint using STSADM
- Restore SharePoint using STSADM
- PowerShell and STSADM Backup Commands

Related Articles

- How to Create a Pre- or Post-Agent Backup Command Batch File or Script
- Configuring a Replication Destination
- Backing Up Using PowerShell and STSADM

Additional Resource

- Back up a farm configuration (SharePoint Foundation 2010)
- SharePoint Governance and Manageability
- Backup: Stsadm operation (Office SharePoint Server)

You can back up Microsoft SharePoint databases using Barracuda Backup for storage. The Barracuda Backup Agent provides a complete backup of Windows SharePoint Services (WSS).

> ⚠ **Important**
> Do not use other methods to back up Microsoft SharePoint databases, such as Microsoft or third-party utilities, when using the Barracuda Backup Agent. If you use more than one back up method on the same database, one or more of those methods may cause truncation of the transaction logs. This forces a full backup of the database every time, and can result in data that cannot be restored.
>
> If you wish to run pre or post Barracuda Backup Agent commands, you can edit the bbconfig.ini file. For details, refer to How to Create a Pre- or Post-Agent Backup Command Batch File or Script.

To perform a consistent restore of the WSS, ensure that the following components are included in the SharePoint back up; if you select the entire system, the backup automatically includes all of these components:

- **Windows SharePoint Services Installation Directory** - This directory and its sub directories contain WSS installation and configuration files including binaries, site templates, style sheets, customization information for site definitions, etc.
- **Microsoft Internet Information (IIS) Virtual Servers** - WSS uses one or more virtual servers to host websites. In SharePoint 2003 and WSS 2.0 the entire configuration for the IIS website is stored in the configuration and content databases.

  > ⓘ **SharePoint 2003/WSS 2.0**
  > In SharePoint 2003 and WSS 2.0 the entire configuration for the IIS website is stored in the configuration and content databases.

- **Windows SharePoint Services Databases** - By default WSS installs a Microsoft SQL Server Desktop Engine/SQL Server Embedded Edition (WMSDE/SSEE) called SHAREPOINT or Microsoft SSEE and creates a configuration and content database.
- **Usage Analysis Logs** - Enable usage analysis logging to generate daily WSS log files to track website usage.

Install the Barracuda Backup Agent

Use the following steps to install the Barracuda Backup Agent (Windows) on the SharePoint server:

1. Log in to the Barracuda Backup web interface, and select the associated Barracuda Backup Server in the left pane.
2. Go to the **SYSTEM > Software Downloads** page, and download the **Barracuda Backup Agent (Windows)** to each SharePoint server you want to back up.
3. Once downloaded, install the Agent.

Add SharePoint as a Data Source

Use the following steps to add the SharePoint database as a data source:

1. Log in to the Barracuda Backup web interface, and go to the **BACKUP > Sources** page.
2. Click **Add Computer**, and enter the details for your SharePoint database, and click **Save**.
3. In the **Data Sources** page, select **Barracuda Agent Software** as the **Data Type**, and fill in the details for the SharePoint database.
4. Click **Test Software Connectivity** to verify the Barracuda Backup Server can connect to the Agent installed on the SharePoint server.
5. In the **Items Selection** section, click **Select All Items** to back up the entire database, or click **Select Specific Items** to select individual items for backup.
6. To back up to Barracuda Cloud Storage, turn on **Replicate to Barracuda Cloud Storage**.

Backup Schedules
To replicate to another Barracuda Backup Server, refer to Configuring a Replication Destination.

7. Click **Save**.

Backup Tasks
Once you add the SharePoint database as a data source, complete the following data backup tasks:

- Task 3: Create Backup Schedules
- Task 4: Create Data Retention Policies
- Task 5: Modify Your Back Up Rate Limit (Optional)
- Task 6: Exclude Files from a Backup (Optional)
- Task 7: Create Rules to Watch Important Backup Files (Optional)
- Task 8: Check Backup Reports

SharePoint Backup Considerations

In SharePoint 2007 and WSS 3.0 you must stop the server farm to create a valid backup. The built-in tools do not recover these databases when restoring a server farm due to data synchronization issues with other SharePoint databases.

In SharePoint 2010 and higher you can backup and restore a server farm configuration. For more information, refer to the Microsoft SharePoint TechNet article Back up a farm configuration (SharePoint Foundation 2010). In SharePoint 2010 and higher you can back up the configuration database in PowerShell using the `Backup-SPConfigurationDatabase` command or `Backup-SPFarm` with the `SPConfigurationOnly` switch.

Important
You can only restore to a SharePoint environment with the *same* configuration.

Site Recycle Bin

In SharePoint 2010 SP1 and higher the Administrator can use the **Site Recycle Bin** to create a snapshot of subscriptions and site collections deleted through the SharePoint user interface or SharePoint tools. For more information, including set up instructions, refer to SharePoint Governance and Manageability. Additionally, refer to this article for details on adding similar functionality in SharePoint 2007 and WSS 3.0.

SharePoint Backup Best Practices

Schedule routine SharePoint server farm backups for consistent configuration and Central Administrator database recovery using the following steps:

1. Log into the server running SharePoint Central Administration, open **Microsoft SQL Server Management Studio**.
2. Navigate to **Services and Applications > Services**, and stop the following services:

SharePoint 2010	SharePoint 2007	WSS 3.0
SharePoint 2010 Administration	Microsoft Single Sign-On	Windows SharePoint Services Administration
SharePoint 2010 Timer	Office Document Conversions Launcher	Windows SharePoint Services Search
SharePoint 2010 Tracing	Office SharePoint Server Search	Windows SharePoint Services Timer
SharePoint 2010 User Code Host	Windows SharePoint Services Administration	Windows SharePoint Services Tracing
SharePoint 2010 VSS Writer	Windows SharePoint Services Search	Windows SharePoint Services VSS Writer
SharePoint Foundation Search	Windows SharePoint Services Timer	
World Wide Web Publishing Service	Windows SharePoint Services Tracing	
SharePoint Server Search	Windows SharePoint Services VSS Writer	

Web Analytics Data Processing Service		
Web Analytics Web Service		

3. At a command prompt, enter the following command, and then press **Return**:
   ```
   iisreset /stop
   ```
4. Use the Barracuda Backup Agent to back up the server farm Configuration, Central Administration, Service Applications and Search databases.
5. At a command prompt, enter the following command, and then press **Return**:
   ```
   iisreset /start
   ```
6. Start the following services:

SharePoint 2010	SharePoint 2007	WSS 3.0
SharePoint 2010 Administration	Microsoft Single Sign-On	Windows SharePoint Services Administration
SharePoint 2010 Timer	Office Document Conversions Launcher	Windows SharePoint Services Search
SharePoint 2010 Tracing	Office SharePoint Server Search	Windows SharePoint Services Timer
SharePoint 2010 User Code Host	Windows SharePoint Services Administration	Windows SharePoint Services Tracing
SharePoint 2010 VSS Writer	Windows SharePoint Services Search	Windows SharePoint Services VSS Writer
SharePoint Foundation Search V4	Windows SharePoint Services Timer	
World Wide Web Publishing Service	Windows SharePoint Services Tracing	
SharePoint Server Search 14	Windows SharePoint Services VSS Writer	
Web Analytics Data Processing Service		
Web Analytics Web Service		

7. Document any other configuration settings and customization for use if you need to recreate the configuration and Central Administration databases in the future.
   - You can export your alternate access mapping (AAM) settings to a text file using the `stsadm -o enumalternatedomains` command. You can then back up this file on the same schedule as the server farm.
   - You can export Information Management Policies to an XML file through the Site Collection home page.

Backing Up SharePoint using STSADM

Use the following steps to back up a SharePoint database using STSADM:

1. Create a backup folder on the server, for example, add a folder to drive **F:**
   F:\backup
2. Go to **Start > Run > cmd**, and at the command prompt, enter the following to change the directory to the SharePoint BIN folder, and then press **Return**:
   ```
   cd C:\program Files\Common Files\Microsoft Shared\web server\extensions\12\BIN
   ```

   > The folder '12' refers to SharePoint 2007; for SharePoint 2003, replace '12' with '11', and for SharePoint 2010, replace '12' with '14'.

3. At the command prompt, enter the `stsadm.exe` command followed by the content location you wish to back up and the location and filename to which you wish to back up, and then press **Return**.
   To back up the site collection, use the `url` parameter:
   ```
   stsadm.exe -o backup -url <location of the site to back up> -filename <backup location>.dat
   ```

   For example:
   ```
   stsadm.exe -o backup -url https://sharepointserver:8090 - filename "F:\backup\Sharepointbackup .dat"
   ```

For a full or differential back up of an individual database, web application, or the entire SharePoint farm, use the `backupmethod` parameter:

```
stsadm.exe -o backup -directory <directory path> -BackupMethod [Full | Differential] -Item <content
path >
```

4. Allow the backup to complete.
5. Go to the location where you backed up your content; the backup file should display in the folder.

> **Additional Information**
> For more information on STSADM back up operations, refer to the Microsoft TechNet article Backup: Stsadm operation (Office SharePoint Server).
>
> See Backing Up Using PowerShell and STSADM for STSADM commands to back up specific types of content in a SharePoint server farm.

Restore SharePoint using STSADM

Use the following steps to restore a SharePoint database using STSADM:

1. On the SharePoint server, go to **Start > Run > cmd**, and at the command prompt, change the directory to the SharePoint BIN folder, and then press **Return**:
2.
   ```
   cd C:\program Files\Common Files\Microsoft Shared\web server\extensions\12\BIN
   ```

> The folder '12' refers to SharePoint 2007; for SharePoint 2003, replace '12' with '11', and for SharePoint 2010, replace '12' with '14'.

3. At the command prompt, enter the `stsadm.exe` command followed by the `restore` and `overwrite` parameters, and the location you wish to restore and from where you wish to restore, and then press **Return**:
   ```
   stsadm.exe -o restore -url <location of the site to restore> -filename <backup location>.dat
   -overwrite
   ```

   For example:
   ```
   stsadm.exe -o backup -url https://sharepointserver:8090 -filename "F:\backup\Sharepointbackup.dat"
   -overwrite
   ```
4. This overwrites the site with the backed up content.

> **Backup Tasks**
> Once you add the SharePoint database as a data source, complete the following data backup tasks:
>
> - Task 3: Create Backup Schedules
> - Task 4: Create Data Retention Policies
> - Task 5: Modify Your Back Up Rate Limit (Optional)
> - Task 6: Exclude Files from a Backup (Optional)
> - Task 7: Create Rules to Watch Important Backup Files (Optional)
> - Task 8: Check Backup Reports

PowerShell and STSADM Backup Commands

In addition to the Barracuda Backup Agent, you can back up using PowerShell and STSADM.

Click here to expand...

Content Database Backup - PowerShell Command

At a command prompt enter the following command, and then press **Return**:

```
Backup-SPFarm -Directory -BackupMethod [Full | Differential] -Item [-Verbose]
```

Content Databases Backup - STSADM Command

At a command prompt, enter the following command, and then press **Return**:

```
stsadm.exe -o backup -directory "F:\SharePointBackup" -backupmethod [Full | Differential] -overwrite
-item databasename
```

Site Collection Backup - PowerShell Command

Site Lock
For a site collection, you must manage the site lock to block updates or deletions to the site collection during a backup.

At a command prompt enter the following command, and then press **Return**:

```
Backup-SPSite -Identity -Path [-Force] [-NoSiteLock] [-UseSqlSnapshot] [-Verbose]
```

Site Collection Backup - STSADM Command

At a command prompt, enter the following command, and then press **Return**:

```
stsadm.exe -o setsitelock -url url_of_sitecollection -lock readonly
```

```
stsadm.exe -o backup -filename "F:\SharePointBackup\filename_for_sitecollection" -overwrite -url
sitecollection_url
```

```
stsadm.exe -o setsitelock -url sitecollection_url -lock none
```

Export Site, List or Document Library Backup - PowerShell Command

At a command prompt enter the following command, and then press **Return**:

```
Export-SPWeb -Identity -Path [-ItemUrl ] [-IncludeUserSecurity] [-IncludeVersions] [-NoFileCompression]
[-GradualDelete] [-Verbose]
```

Export Site Backup - STSADM Command

At a command prompt enter the following command, and then press **Return**:

```
stsadm -o export -url -filename [-overwrite] [-includeusersecurity] [-haltonwarning] [-haltonfatalerror]
[-nologfile] [-versions] <1-4> [-cabsize] [-nofilecompression] [-quiet]
```

Use the `NoFileCompression` parameter to specify no file compression during export to reduce resource usage.

Service Application and Shared Services Provider Backup - PowerShell Command

At a command prompt enter the following command, and then press **Return**:

```
Backup-SPFarm -Directory -BackupMethod [Full | Differential] -Item [-Verbose]
```

Service Application and Shared Services Provider Backup - STSADM Command

At a command prompt enter the following command, and then press **Return**:

```
stsadm -o backup -directory F:\backup -backupmethod [Full | Differential] -item SSP_NAME
```

Web Application Backup - PowerShell Command

At a command prompt enter the following command, and then press **Return**:

```
Backup-SPFarm -Directory -BackupMethod [Full | Differential] -Item [-Verbose]
```

Web Application Backup - STSADM Command

At a command prompt enter the following command, and then press **Return**:

```
stsadm.exe -o backup -directory "F:\SharePointBackup" -backupmethod [Full | Differential] -overwrite
-item web_application_name
```

Understanding IBM Domino Server Backup

This article refers to Barracuda Backup firmware 3.0 and higher.

The Barracuda Backup Agent does not support IBM® Domino ® or IBM Notes ®, however, the Barracuda Backup Agent (Windows) protects IBM Domino databases on a Microsoft ® Windows® 2003 or Windows 2008 platform using File System backup. Barracuda Backup does not support IBM Domino transaction logging.

In this article:

- IBM Domino Server Databases
- IBM Domino Server Backup
- Windows Volume Shadow Copy Service

Related Articles

- Create a Pre- or Post Agent Backup Command Batch File

Additional Resource

Barracuda Networks knowledgebase solution #00005950

An IBM Domino server is a collection of databases using a flat file structure. A review of the database files in an IBM Domino environment reveals that each user has a unique database for email, and that they may share application databases. This can result in hundreds or even thousands of smaller, unique database files in the IBM Notes **/data** directory. In comparison, an Exchange deployment has relatively few databases supporting an entire organization.

IBM Domino Server Databases

IBM Domino databases are accessed using IBM Notes clients. Within the database file there can be data, design elements, and programming code, and each database file has its own security in the form of an Access Control List (ACL). A IBM Domino database has a file extension of **.nsf** .

IBM Domino Server Backup

A complete backup of an IBM Domino Server includes:

1. IBM Domino Server data files
2. All databases
3. Template files
4. Notes.ini file
5. ID files

⚠ Before you begin a backup, verify the following files are open and running on the IBM Domino Server:

- Logs.nsf
- names.nsf
- mail.box
- Server ID file

Windows Volume Shadow Copy Service

Through the use of the Windows Volume Shadow Copy Service (VSS), the Barracuda Backup Service can consistently capture the open database files. Using VSS, the Barracuda Backup Service can perform both full and incremental backups of the IBM Domino server. Because the data may be made up of many small database files that can change daily, the incremental/differential backup can be very close to the master database in size. Due to the manner in which IBM Domino writes the changes to the end of the files, a large amount of deduplication occurs on these backups.

When using the VSS backup method, it is recommended that you execute the following two commands prior to the backup:

- `nserver -c` "drop all"
- `nserver -c` "dbcache flush"

This releases all open sessions and closes most open files. See How to Create a Pre- or Post-Agent Backup Command Batch File or Script if you wish to create a pre-backup command batch file.

How to Create a Pre- or Post-Agent Backup Command Batch File or Script

> This article refers to firmware 5.3 and higher. This articles applies to the Barracuda Backup Agent (Windows) and BarracudaBackup Agent (Linux) .

In this article:

- Barracuda Backup Agent Running on a Microsoft Windows System
    - Stop a Process
    - Start a Process
- Barracuda Linux Backup Agent Running on a Linux/Unix-Based System

Related Articles

- Understanding IBM Domino Server Backup
- How to Restore from Local and Offsite Backups
- Barracuda Backup Agent

Barracuda Backup Agent Running on a Microsoft Windows System

You can run a pre- or post-Agent backup command batch file by editing the `bbconfig.ini` file. This enables you to stop and start certain processes on the host computer where the Barracuda Backup Agent (Windows) is installed. This can allow you to stop conflicting processes during the time that the Agent is backing up files.

Stop a Process

To automatically stop a specific process before starting the backup job, you can specify the batch file to stop the service.

1. Navigate to the `bbconfig.ini` file on the server in the following location:
   `C:\Program Files\Barracuda\Barracuda Backup Agent\config\`
2. Open the `bbconfig.ini` file in a text editor, and in the [**configuration**] section, add two lines like:
   ```
   # the batch file to stop the process
   preExecuteScript=c:\stop.bat
   ```
3. Save and close the file.

Start a Process

To automatically start a specific process after completing the backup job, you can specify the batch file to start the service.

1. Navigate to the `bbconfig.ini` file on the server in the following location:
   `C:\Program Files\Barracuda\Barracuda Backup Agent\config\`
2. Open the `bbconfig.ini` file in a text editor, and in the [**configuration**] section, add two lines like:
   ```
   # the batch file to start the process
   postExecuteScript=c:\start.bat
   ```
3. Save and close the file.

> ⓘ If the pre-backup batch commands fail, the backup may not run.

Barracuda Linux Backup Agent Running on a Linux/Unix-Based System

You can run a pre- and post-Agent backup command script by editing the Linux `bbconfig.ini` file to run pre- or post-commands to stop and start certain processes on the Linux/Unix-based system where the Barracuda Backup Agent (Linux) is installed, For example, `script.sh:`

1. Navigate to the `bbconfig.ini` file on the system where the Barracuda Linux Backup Agent is installed.
2. Open the `bbconfig.ini` file in a text editor, and below the [**configuration**] section, enter:
    - `preExecuteScript=/root/script.sh`
    - `postExecuteScript=/root/script.sh`
3. Save and close the file.

How to Configure GroupWise Message-Level Backups

This article refers to Barracuda Backup firmware 4.2 and higher, and Novell® NetWare® Server and GroupWise™.

In this article:

- Requirements
- Configure the GroupWise Server
- Generate a GroupWise Trusted Key
- Add the GroupWise Server as a Data Source
- Retain Emails

Related Articles

- How to Restore Exchange and GroupWise Messages

Additional Resource

- GroupWise Administration Guide

Set up your Novell NetWare Server to complete GroupWise message-level backups with a Barracuda Backup Server.

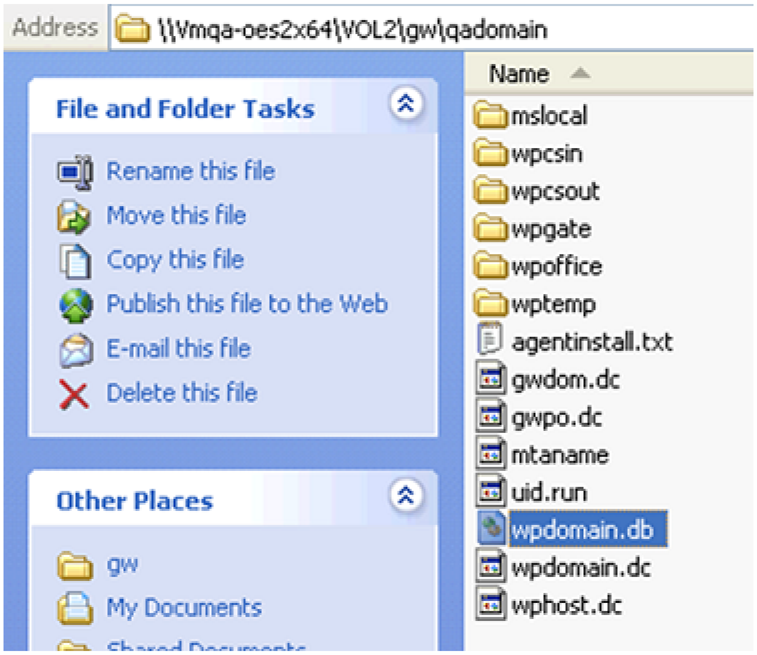
Requirements

- NetWare Server 6.5 or greater
- GroupWise Server version 8 or greater

Configure the GroupWise Server

Use the following steps to configure the GroupWise Server:

1. On a Microsoft® Windows® workstation where the Novell Client is installed, log in with an account that has access to the GroupWise primary domain database file **wpdomain.db**:


Address
\\Vmqa-oes2x64\VOL2\gw\qadomain
File and Folder Tasks
Rename this file
Move this file
Copy this file
Publish this file to the Web
E-mail this file
Delete this file
Other Places
gw
My Documents
Name
mslocal
wpcsin
wpcsout
wpgate
wpoffice
wptemp
agentinstall.txt
gwdom.dc
gwpo.dc
mtaname
uid.run
wpdomain.db
wpdomain.dc
wphost.dc

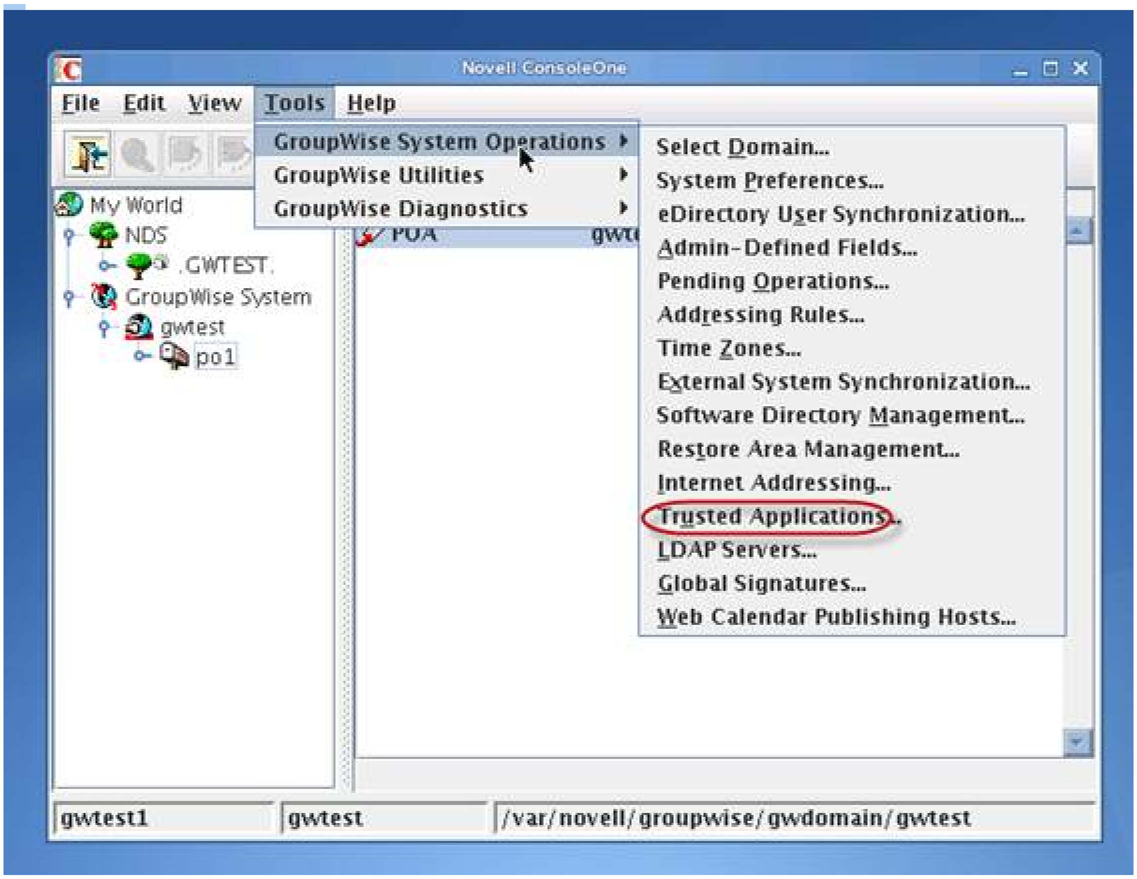
2. Create an account to be used by the Barracuda Backup Server to access the email in each mailbox; the service account must be a member of either the **Enterprise Administrators** or **Domain Administrators** group.

Generate a GroupWise Trusted Key

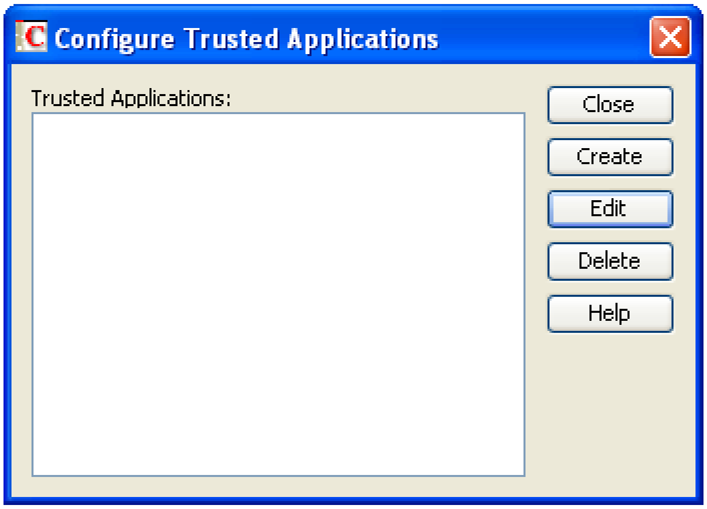
A trusted application key allows a third-party program to authenticate to the post office agent (POA) or the Internet Agent and obtain GroupWise information that would otherwise be available only by logging in to GroupWise mailboxes. Starting with GroupWise 8 Support Pack 1, you can create a trusted application and its associated key in ConsoleOne for use with both Linux and Windows trusted applications.

Use the following steps to generate a trusted key:

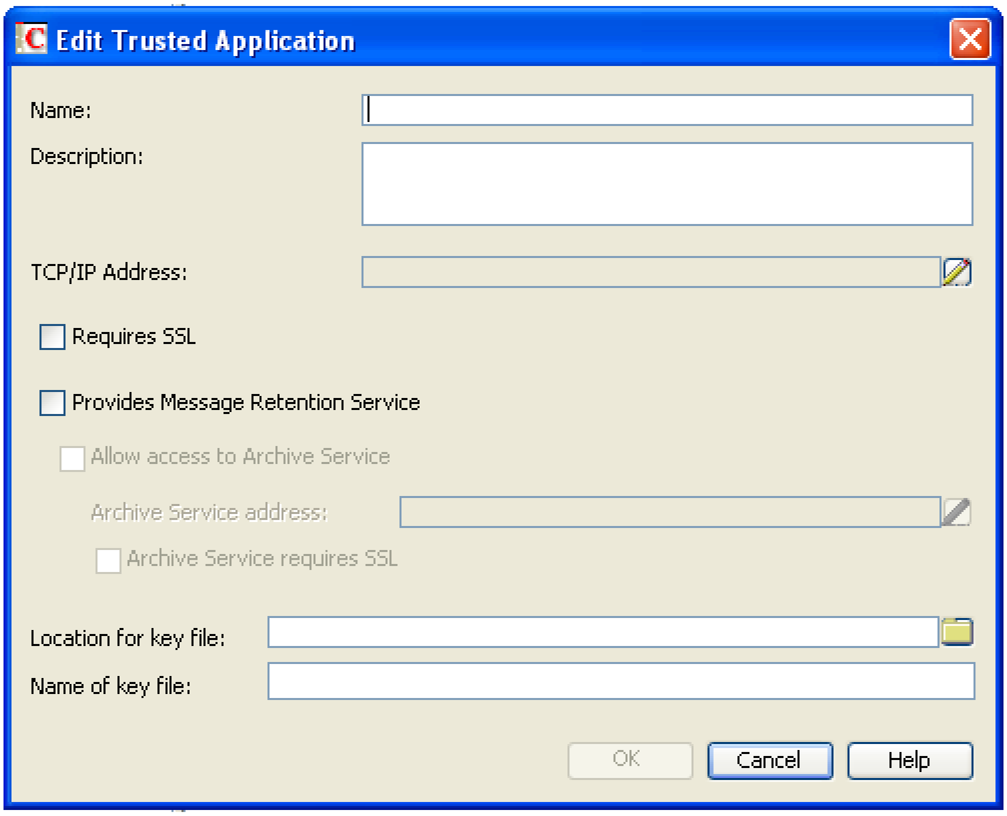
1. Open ConsoleOne. From the **Tools** menu, point to **GroupWise System Operations**, and click **Trusted Applications**:


Novell ConsoleOne
File
Edit
View
Tools
Help
GroupWise System Operations
GroupWise Utilities
GroupWise Diagnostics
My World
NDS
.GWTEST.
GroupWise System
gwtest
po1
POA
Select Domain...
System Preferences...
eDirectory User Synchronization...
Admin-Defined Fields...
Pending Operations...
Addressing Rules...
Time Zones...
External System Synchronization...
Software Directory Management...
Restore Area Management...
Internet Addressing...
Trusted Applications...
LDAP Servers...
Global Signatures...
Web Calendar Publishing Hosts...
gwtest1
gwtest
/var/novell/groupwise/gwdomain/gwtest

2. The **Configure Trusted Applications** dialog box displays. Click **Create**:


Configure Trusted Applications
Trusted Applications:
Close
Create
Edit
Delete
Help

3. The **Edit Trusted Application** dialog box displays:



4. In the **Name** field, type `BitLeap Backup`, and enter a description for the trusted application in the **Description** field.
5. Leave the **TCP/IP Address** field blank to allow the trusted application from any server, or, to restrict the location from which the trusted application can run, click the **Edit** icon to the right of the field, and in the **Edit Network Address** dialog box, specify the IP address or DNS hostname of the trusted application server. Click **OK** to save your settings and close the dialog box.
6. To require a secure (SSL) connection between the trusted application, POAs, and Internet Agents, select the **Requires SSL** check box.
7. Click the **Browse** icon to the right of the **Location for key file** field, and browse to and select the directory where you want to create the trusted application key file.
8. In the **Name of Key File** field, enter the trusted application key file name.
9. Click **OK** to save the trusted application configuration information.

Add the GroupWise Server as a Data Source

1. Log in to Barracuda Backup web interface, and select the associated Barracuda Backup Server in the left pane.
2. Go to the **BACKUP > Sources** page, and click **Add Computer**; the **Add Computer** page displays.
3. In the **Computer Information** section, enter the Netware Server description and hostname or IP address.
4. From the **Computer Type** drop-down menu, select **Novell**.
5. In the **Novell Computer Information** section, enter the Server username and password credentials.
6. Click **Save**.
7. On the **Add Data Source** page, enter a description for the data source, and from the **Data Type** drop-down menu, select **Message-Level Backup (GroupWise)**.
8. In the **Message-Level Backup (GroupWise) Information** section, enter the GroupWise mailbox location in the **Base Context** field.
9. In the **Trusted Application Key** field, paste the Trusted Application Key created in the previous section.
10. You can optionally enter the e-Directory Server hostname or IP address.
11. Click the **Test GroupWise Connectivity** to verify the connection.
12. Once the connection is verified, select the mailboxes you wish to backup.
13. Click **Save**.

Retain Emails

This step is optional. You can optionally set up GroupWise to have all emails backed up by Barracuda Networks. This feature instructs GroupWise to not purge emails until Barracuda Backup has a backup copy of the email. For information on how to set up this feature, please view the Group Wise Administration Guide - Environment Options: Retention section available on the Novell website.

How to Set Up a Root Account to Back Up Macintosh OS X

This article refers to Barracuda Backup firmware version 5.0 or higher, and Macintosh OS X.

In this article:

- Create a Root Account
- Log in as the Root User
- Set up SSH Key for Mac

Additional Resource

- Enabling and using the "root" user in Mac OS X

By default, the root account on Macintosh OS X Servers is disabled. If a user uses the admin account to back up content to Barracuda Backup, they may encounter a warning message stating that some files cannot be backed up. To resolve this issue, Barracuda Networks recommends using the root account for backups as the root account has full permission on the disk and is able to back up the server with limited warnings.

Create a Root Account

Set up a root account based on your software release.
OS X Lion

1. From the **Apple** menu, click **System Preferences**.
2. From the **View** menu, click **Users & Groups**.
3. Click the lock and authenticate as an administrator account.
4. Click **Login Options**, and click **Edit** at the bottom right of the screen.
5. Click **Open Directory Utility**, and in the **Directory Utility**, click the lock.
6. Enter the administrator account name and password, and click **OK**.
7. From the **Edit** menu, click **Enable Root User**.
8. Enter the root password you wish to use in both the **Password** and **Verify** fields, and click **OK**.

Mac OS X v10.6.x

1. From the **Apple** menu, click **System Preferences**.
2. From the **View** menu, click **Accounts**.
3. Click the lock and authenticate as an administrator account.
4. Click **Login Options**, and click **Edit** at the bottom right of the screen.
5. Click **Open Directory Utility**, and in the **Directory Utility**, click the lock.
6. Enter the administrator account name and password, and click **OK**
7. From the **Edit** menu, click **Enable Root User**.
8. Enter the root password you wish to use in both the **Password** and **Verify** fields, and click **OK**.

Mac OS X v10.5.x

1. From the **Finder's Go** menu, choose **Utilities**, and open **Directory Utility**.
2. Click the lock in the **Directory Utility** window.
3. Enter an administrator account name and password, and click **OK**.
4. From the **Edit** menu, click **Enable Root User**.
5. Enter the root password you wish to use in both the **Password** and **Verify** fields, and click **OK**.

Mac OS X v10.4.x or earlier

1. Click the **Finder** icon in the **Dock**.
2. From the **Go** menu, click **Applications**.
3. Open the **Utilities** folder.
4. Open the **NetInfo Manager** utility.
5. Click the lock in the **NetInfo Manager** window.
6. Enter the administrator account name and password, and click **OK**

Mac OS X 10.2 and Later

For Mac OS X 10.2 and later, choose **Enable Root User** from the **Security** menu.
Mac OS X 10.0 and 10.1

1. From the **Domain** menu, point to **Security**, and click **Enable Root User**.
2. If you have not previously set a root password, an alert box displays the message **NetInfo Error**, indicating that the password is blank. Click **OK**.
3. Enter the root password you wish to use, and click **Set**.

4. Enter the password again, and click **Verify**.
5. Click the lock to prevent changes.

Log in as the Root User

Log in using the root account based on your software release.
Mac OS X v10.2 or Later

1. If you are logged in, choose **Log Out** from the **Apple** menu.
2. If you are logging in from a list of usernames with pictures, click **Other**.
3. In the **Name** field, type: `root`
4. In the **Password** field, type the password you defined earlier.

Mac OS X v10.0 to v10.1.5

> ⓘ After enabling the root user, you must log out from Mac OS X and log back in as the root user. Logging in to Mac OS X from a list of usernames is the default behavior for later versions of Mac OS X. Logging in by typing your username in a text entry field is the default behavior in earlier versions of Mac OS X. You can choose either method in **Login** preferences. The root user does not appear in the list, so you need the text entry option. If necessary, follow these steps to change the login method to text entry:
>
> 1. From the **Apple** menu, click **System Preferences**.
> 2. From the **View** menu, click **Login**.
> 3. Click the **Login Window** tab.
> 4. Select **Name and password entry fields**, and complete the steps in the next section to log in as root account.

1. If you are logged in, choose **Log Out** from the **Apple** menu.
2. In the **Name** field, type: `root`
3. In the **Password** field, type the password you defined earlier.

Set up SSH Key for Mac

For each local Barracuda Backup Server, identify the data sources that are to be backed up. There may be more than one data source on each server, and each can have unique backup characteristics.

1. Log in to the Barracuda Backup web interface, and select the associated Barracuda Backup Server in the left pane.
2. Go to the **BACKUP > Sources** page, and click **Add Computer** to identify the computer.
3. Enter the IP address of the Mac Server.
4. From the **Computer Type** drop-down menu, select **Mac OS X**.
5. In the **Mac OS X Information** section, enter `root` in the **Username** field.
6. Download the SSH Key installer, and run the setup.
7. Once the key is installed, save the settings. Click **Save** in the web interface.
8. In the **Add Data Source** page, enter the remaining system details.
9. In the **Folder Selection** section, you can **Select All Folders** for backup, or click **Pick Certain Folders** to specify individual folders for backup.
10. Click **Save**.

How to Back Up Linux/UNIX Data Using SSHFS

> This article refers to Barracuda Backup firmware 4.3 and higher. Barracuda Backup uses the SSH Filesystem (SSHFS) and public key authentication to connect and back up Linux data.

In this article:

- Add the Linux Server
- Add Linux Server Data Sources
- Set Up Backup Schedules and Retention Policies

Related Articles
- Barracuda Backup Agent (Linux)

Additional Resource
- Ubuntu OpenSSH Server sshd Installation

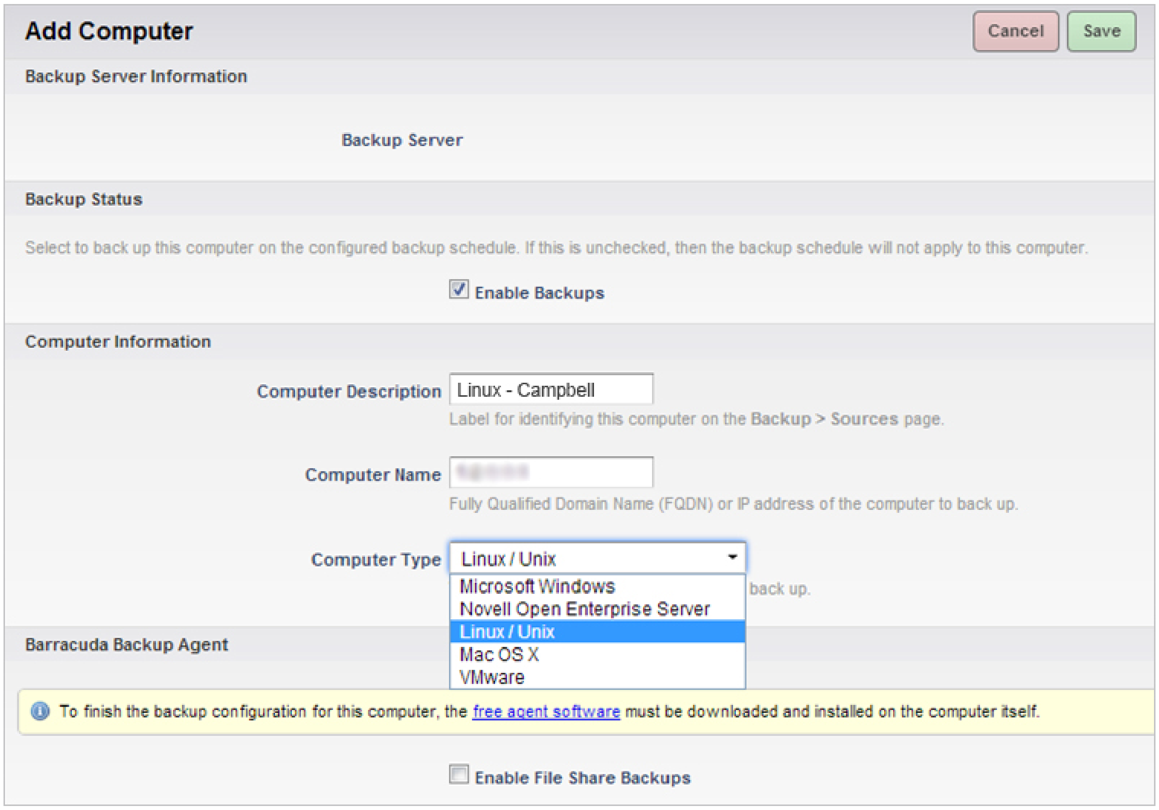
> **Backed Up Content**
> This article describes how to back up Linux/UNIX-based file systems, such as Red Hat, Ubuntu, or SUSE, using SSHFS. Before backing up data, verify that you have adequate permissions to the folder you intend to back up. Note that SSHFS cannot back up open or locked files.

Add the Linux Server

Use the following steps to add the Linux Server to Barracuda Backup.

> Before adding the Linux Server to Barracuda Backup, notify users that their Secure Shell (ssh) session may be lost during set up.

1. Log in to the Barracuda Backup web interface, and select the associated Barracuda Backup Server in the left pane.
2. Go to the **BACKUP > Sources** page, and click **Add Computer**.
3. Enter a computer description and enter the IP address or fully qualified domain name in the **Computer Name** field.
4. From the operating system drop-down menu, select **Linux / Unix**:


Add Computer
Cancel
Save
Backup Server Information
Backup Server
Backup Status
Computer Information
Microsoft Windows
Novell Open Enterprise Server
Linux / Unix
Mac OS X
VMware
Barracuda Backup Agent

Select to back up this computer on the configured backup schedule. If this is unchecked, then the backup schedule will not apply to this computer.

☑ Enable Backups

Computer Description: Linux - Campbell
Label for identifying this computer on the **Backup > Sources** page.

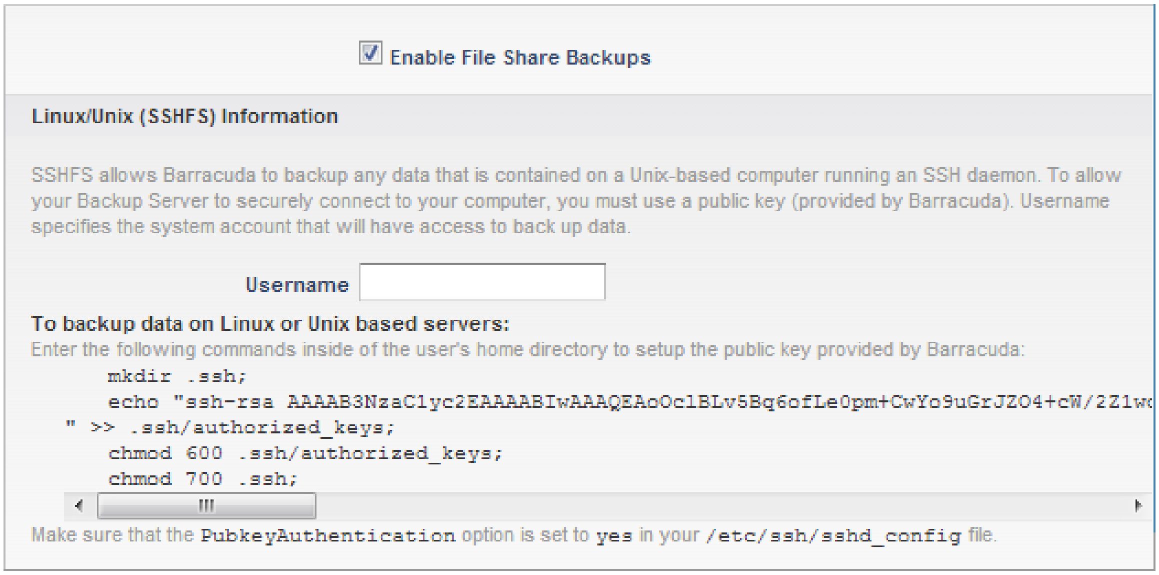
Computer Name: [redacted]
Fully Qualified Domain Name (FQDN) or IP address of the computer to back up.

Computer Type: Linux / Unix

To finish the backup configuration for this computer, the free agent software must be downloaded and installed on the computer itself.

☐ Enable File Share Backups

5. Turn on **Enable File Share Backups**; the **Linux/Unix (SSHFS) Information** section displays:



☑ Enable File Share Backups

Linux/Unix (SSHFS) Information

SSHFS allows Barracuda to backup any data that is contained on a Unix-based computer running an SSH daemon. To allow your Backup Server to securely connect to your computer, you must use a public key (provided by Barracuda). Username specifies the system account that will have access to back up data.

Username

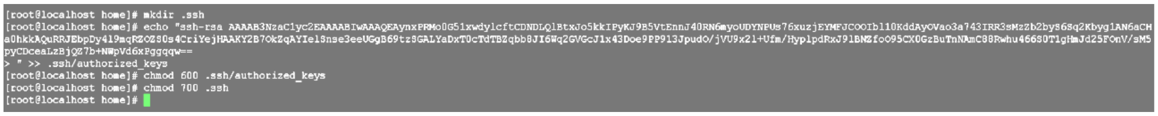
To backup data on Linux or Unix based servers:

Enter the following commands inside of the user's home directory to setup the public key provided by Barracuda:

```
     mkdir .ssh;
     echo "ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAoOc1BLv5Bq6ofLe0pm+CwYo9uGrJZO4+cW/2Z1w
  " >> .ssh/authorized_keys;
     chmod 600 .ssh/authorized_keys;
     chmod 700 .ssh;
```

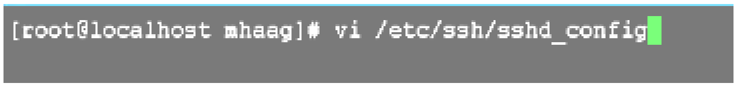
Make sure that the `PubkeyAuthentication` option is set to `yes` in your `/etc/ssh/sshd_config` file.

6. Enter the **Username** for the system account that is to have access to back up data.
7. In the **To backup data on Linux or Unix based servers** section, copy the commands to your clipboard.
8. On the Linux Server, determine the location of the `ssh` directory, including the `authorized_keys` file, in the user's home directory:
    - If a *username different than root is used*, place the `ssh` directory, including the `authorized_keys` file , in the user's home directory.
    - If the *root account is used*, place the `ssh` directory, including the `authorized_keys` file, in the root home directory
9. Log in to the Linux Server using an ssh client such as PuTTY, and paste and run the commands copied in **step 6** into the appropriate directory based on **step 7** to set up the public key provided by Barracuda Networks:



```
[root@localhost home]# mkdir .ssh
[root@localhost home]# echo "ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAynxPRMo0G51xwdylcftCDNDLQlBtxJo5kkIPyKJ9B5VtEnnJ40RN6myoUDYNPUs76xuzjEYMFJCOOIbl10KddAyOVao3a743IRR3sMzZb2byS6Sq2Kbyg1AN6aCH
a0hkkAQuRRJEbpDy419mqRZOZS0s4CriYejHAAKY2B7OkZqAYIel8nse3eeUGgB69tzSGALYaDxT0cTdTBZqbb8JI6Wq2GVGcJ1x43Doe9PP913JpudO/jVU9x21+Ufm/HyplpdRxJ91BNZfoO95CX0GzBuTnNAmC88Rwhu466S0T1gHmJd25FOnV/sM5
pyCDceaLzBjQZ7b+NWpVd6xPggqqw==
> " >> .ssh/authorized_keys
[root@localhost home]# chmod 600 .ssh/authorized_keys
[root@localhost home]# chmod 700 .ssh
[root@localhost home]#
```

10. On the Linux Server, navigate to ***/etc/ssh*** and open the file **sshd_config** :



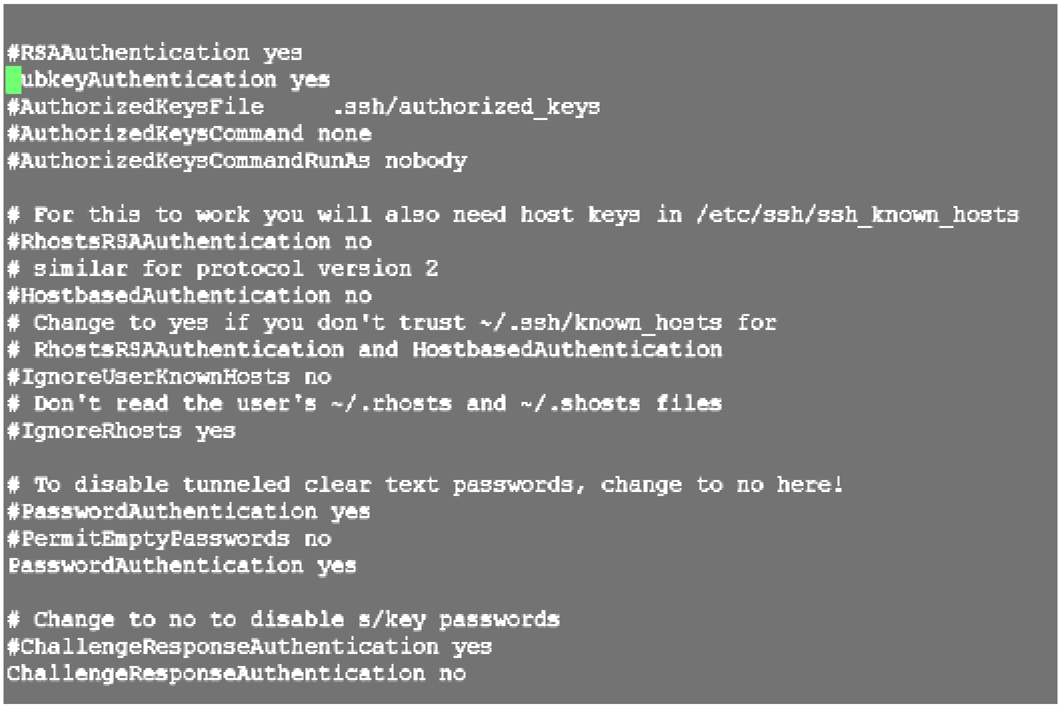
```
[root@localhost mhaag]# vi /etc/ssh/sshd_config
```

If an error message stating that no `sshd_config file could be found` displays, the ssh daemon may not be installed. In some Linux installations, the ssh client is installed without the ssh daemon.

For more information, refer to the documentation available online or included with your version of Linux for the proper procedures to install the ssh daemon on your server. For your reference, the following link is provided to show an example of sshd installation instructions.

https://help.ubuntu.com/10.04/serverguide/openssh-server.html

11. In the file **sshd_config**, locate the line `PubkeyAuthentication yes`, and r emove the pound sign "#":



```
#RSAAuthentication yes
█ubkeyAuthentication yes
#AuthorizedKeysFile     .ssh/authorized_keys
#AuthorizedKeysCommand none
#AuthorizedKeysCommandRunAs nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#RhostsRSAAuthentication no
# similar for protocol version 2
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# RhostsRSAAuthentication and HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
#PermitEmptyPasswords no
PasswordAuthentication yes

# Change to no to disable s/key passwords
#ChallengeResponseAuthentication yes
ChallengeResponseAuthentication no
```

.

12. Run the following command to restart sshd:
    `/etc/init.d/sshd restart`

> Depending on the Linux Server distro, it may be necessary to disable SELinux enforcement using the command:
> `echo 0 > /selinux/enforce`

13. In the Barracuda Backup web interface, click **Save** at the top of the page; the **Add Data Source** page displays.

Add Linux Server Data Sources

Use the following steps to select the Linux Server folders you wish to back up.

1. In the **Add Data Source** page, enter a **Data Description** for the data source.
2. From the **Data Type** drop-down menu, select **File Share - SSHFS** .
3. In the **File Share Information** section, enter the full path of the directory to be backed up in the **Share Name** field, and click **Test Share**; if the connection is successful, a message displays the connection status, for example, **Status: Successfully connected to computer**. If the connection is not successful, return to the **Add Computer** page and verify the IP address is correct before continuing.
4. In the **Folder Selection** section, select **Select All Folders** to back up all data, or select **Pick Certain Folders** to select individual the items for back up.

> **Important**
> If you are backing up `root` or `/`, you must *uncheck* the `proc` and `sys` directories.

5. Click **Save** at the top of the page.

Set Up Backup Schedules and Retention Policies

Once you have your Linux data source items set up for backup, you can set up schedules and retention policies.

Understanding Changed Block Tracking on Virtual Machines

> This article applies to Barracuda Backup Server firmware version 5.0 and higher, and VMware® 4.0 and above with the VMware license which includes access to vSphere® Data Recovery API.

Related Articles

- Enable Changed Block Tracking through the Barracuda Backup Web Interface
- Getting Started with Replication
- Restore a VM to Original Location
- Restore a VM to Alternate VMware Host not available through the Barracuda Backup Service

Additional Resource

- Changed Block Tracking (CBT) on virtual machines
- Enabling Changed Block Tracking (CBT) on virtual machines

Use Changed Block Tracking (CBT) to perform incremental backups on virtual machines running on VMware ESX/ESXi. CBT identifies and tracks block changes since the last backup, and stores these changes in log form, greatly reducing the number of backup windows and improving backup window times. Additionally, subsequent replication efficiency and speed are improved.

> ⓘ Barracuda Backup automatically leverages CBT when CBT is enabled for the virtual machine being backed up.

Setting Up Changed Block Tracking

For details on setting up and enabling CBT on virtual machines, refer to the VMware Knowledge Base articles available from the VMware website:

- Changed Block Tracing (CBT) on virtual machines
- Enabling Changed Block Tracking (CBT) on virtual machines

> ⓘ Contact Barracuda Networks Technical Support for information on enabling CBT from the VMware API.

How to Enable Changed Block Tracking through the Barracuda Backup Web Interface

> This article applies to Barracuda Backup Server firmware version 5.4 and higher, and VMware® 4.0 and above with the VMware license which includes access to vSphere® Data Recovery API.

In this article:

- Requirements
- Enable Changed Block Tracking
- Set Up Changed Block Tracking

Related Articles

- Understanding Changed Block Tracking on Virtual Machines
- Getting Started with Replication
- Restore a VM to Original Location
- Restore a VM to Alternate VMware Host not available through the Barracuda Backup Service

Additional Resource

- Changed Block Tracking (CBT) on virtual machines
- Enabling Changed Block Tracking (CBT) on virtual machines

Use Changed Block Tracking (CBT) to perform incremental backups on virtual machines running on VMware ESX/ESXi. CBT identifies and tracks block changes since the last backup, and stores these changes in log form, greatly reducing the number of backup windows and improving backup window times. In Virtual Machine File system (VMFS) partitions, CBT can identify all disk sectors that are in use. Additionally, subsequent replication efficiency and speed are improved. Barracuda Backup access CBT through the vSphere APIs for Data Protection (VADP) by requesting the changed VMkernel return blocks of data on the virtual disk since the last backup snapshot.

Requirements

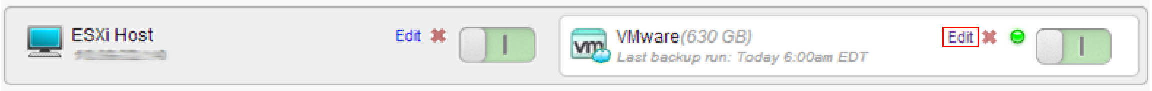
To enable CBT, verify the following is true for your environment:

- The host must be ESX/ESXi 4.1 or later;
- The virtual machine owning the disks to be tracked must be hardware version 7 or later;
- Snapshots exist on the virtual machine; and
- Virtual machine storage is not (persistent or non-persistent) independent disk, therefore it is unaffected by snapshots.

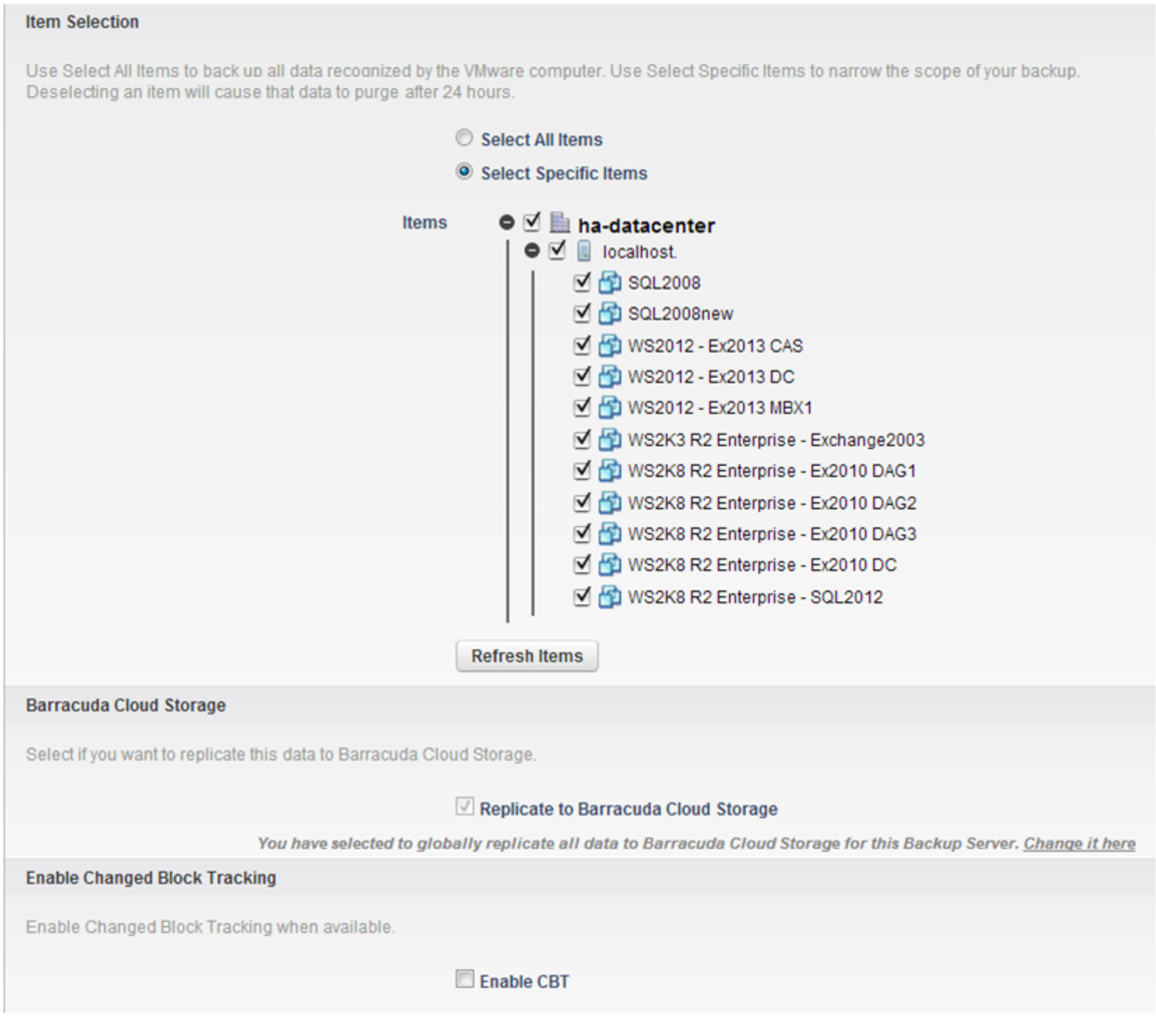
Enable Changed Block Tracking

Use the following steps to enable Changed Block Tracking (CBT) through Barracuda Backup:

1. Log in to Barracuda Backup, and select the associated Barracuda Backup Server in the left pane.
2. Go to the **BACKUP > Sources** page, and click **Edit** next to your VMware data source:



3. Click **Select Specific Items** in the **Item Selection** section, and expand the VMware environment to locate your virtual machines:



Item Selection

Use Select All Items to back up all data recognized by the VMware computer. Use Select Specific Items to narrow the scope of your backup. Deselecting an item will cause that data to purge after 24 hours.

○ Select All Items
● Select Specific Items

Items
- ☑ **ha-datacenter**
  - ☑ localhost.
    - ☑ SQL2008
    - ☑ SQL2008new
    - ☑ WS2012 - Ex2013 CAS
    - ☑ WS2012 - Ex2013 DC
    - ☑ WS2012 - Ex2013 MBX1
    - ☑ WS2K3 R2 Enterprise - Exchange2003
    - ☑ WS2K8 R2 Enterprise - Ex2010 DAG1
    - ☑ WS2K8 R2 Enterprise - Ex2010 DAG2
    - ☑ WS2K8 R2 Enterprise - Ex2010 DAG3
    - ☑ WS2K8 R2 Enterprise - Ex2010 DC
    - ☑ WS2K8 R2 Enterprise - SQL2012

Barracuda Cloud Storage

Select if you want to replicate this data to Barracuda Cloud Storage.

☑ Replicate to Barracuda Cloud Storage

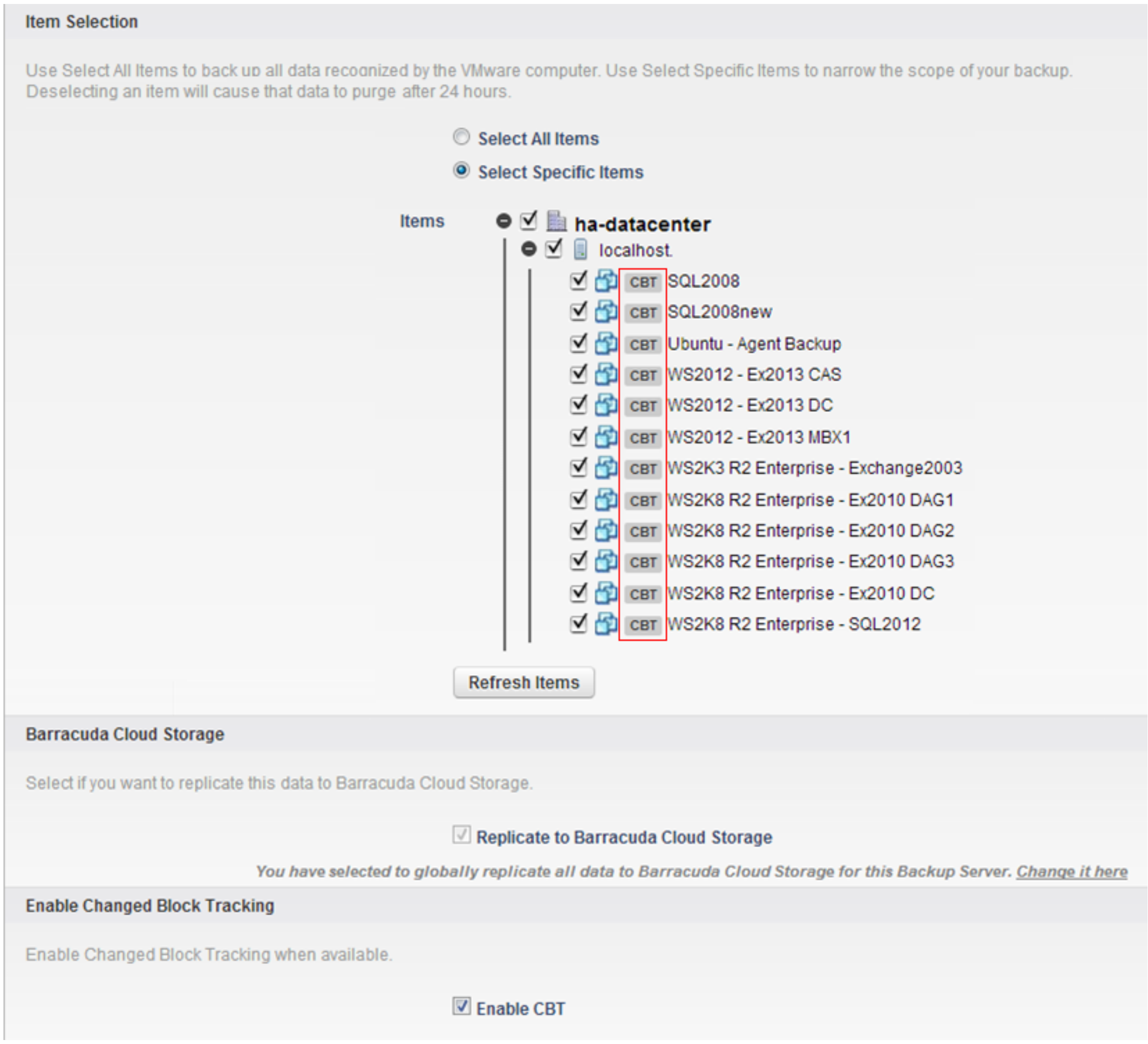
You have selected to globally replicate all data to Barracuda Cloud Storage for this Backup Server. Change it here

Enable Changed Block Tracking

Enable Changed Block Tracking when available.

☐ Enable CBT

4. When **Enable CBT** is turned **On**, **CBT** displays to the left of the virtual machine name:



Item Selection

Use Select All Items to back up all data recognized by the VMware computer. Use Select Specific Items to narrow the scope of your backup. Deselecting an item will cause that data to purge after 24 hours.

○ Select All Items
● Select Specific Items

Items
☑ ha-datacenter
  ☑ localhost
    ☑ CBT SQL2008
    ☑ CBT SQL2008new
    ☑ CBT Ubuntu - Agent Backup
    ☑ CBT WS2012 - Ex2013 CAS
    ☑ CBT WS2012 - Ex2013 DC
    ☑ CBT WS2012 - Ex2013 MBX1
    ☑ CBT WS2K3 R2 Enterprise - Exchange2003
    ☑ CBT WS2K8 R2 Enterprise - Ex2010 DAG1
    ☑ CBT WS2K8 R2 Enterprise - Ex2010 DAG2
    ☑ CBT WS2K8 R2 Enterprise - Ex2010 DAG3
    ☑ CBT WS2K8 R2 Enterprise - Ex2010 DC
    ☑ CBT WS2K8 R2 Enterprise - SQL2012

Refresh Items

Barracuda Cloud Storage

Select if you want to replicate this data to Barracuda Cloud Storage.

☑ Replicate to Barracuda Cloud Storage

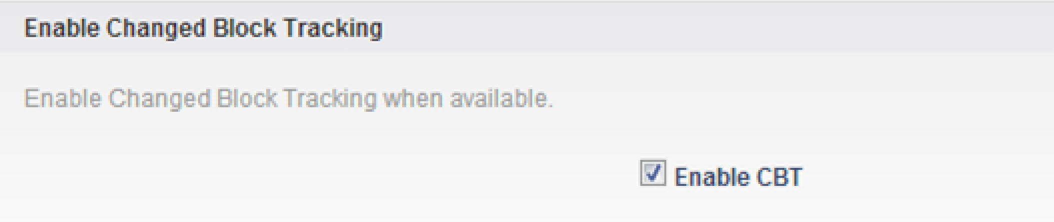
You have selected to globally replicate all data to Barracuda Cloud Storage for this Backup Server. Change it here

Enable Changed Block Tracking

Enable Changed Block Tracking when available.

☑ Enable CBT

5. When **Enable CBT** is turned **Off**, then **CBT** does not display next to the virtual machine name. Click **Enable CBT** to turn enable Changed Block Tracking **On**:



Enable Changed Block Tracking

Enable Changed Block Tracking when available.

☑ Enable CBT

6. Click **Save** to save your backup settings.

Use Changed Block Tracking (CBT) to perform incremental backups on virtual machines running on VMware ESX/ESXi. CBT identifies and tracks block changes since the last backup, and stores these changes in log form, greatly reducing the number of backup windows and improving backup window times. Additionally, subsequent replication efficiency and speed are improved.

> ⓘ Barracuda Backup automatically leverages CBT when it is enabled for the virtual machine being backed up.

Set Up Changed Block Tracking

For details on setting up and enabling CBT on virtual machines, refer to the VMware Knowledge Base articles available from the VMware website:

- Changed Block Tracking (CBT) on virtual machines
- Enabling Changed Block Tracking (CBT) on virtual machines

> ⓘ Contact Barracuda Networks Technical Support for information on enabling CBT from the VMware API.

How to Back Up Network Addressable Storage - NAS

> This article refers to firmware version 4.3 and higher.
>
> In firmware version 5.0 and higher, with CIFS backups, Barracuda Backup is able to back up access control lists (ACLs).

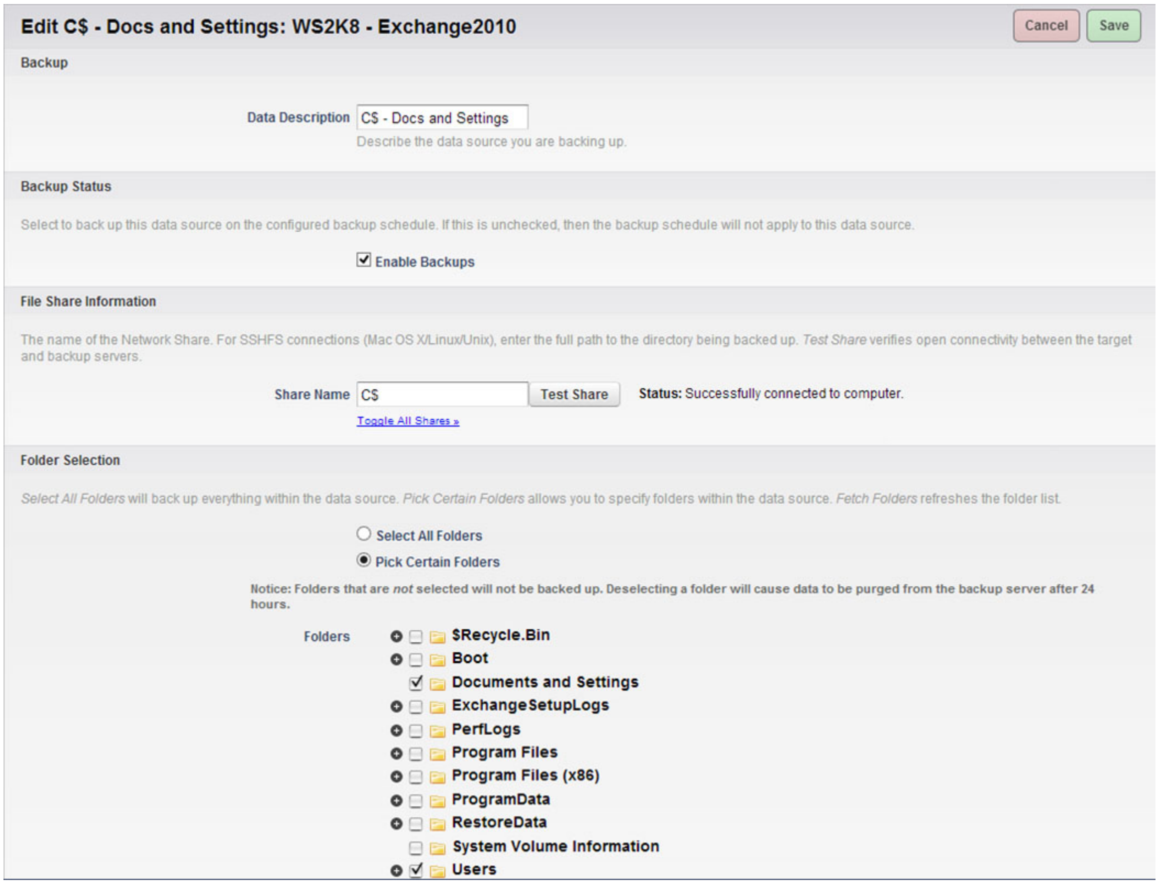
In this article:

- Configure Network Addressable Storage (NAS) Data Sources
- Create Backup Schedules
- Create Data Retention Policies
- Configure Optional Features

Configure Network Addressable Storage (NAS) Data Sources

Use the following steps to identify the data shares on your server that are to be directly backed up:

1. Log into Barracuda Backup, and select the Barracuda Backup Server in the left pane that is to back up the data shares.
2. Go to the **BACKUP > Data Source** page, and click **Add Computer**.
3. In the **Add Computer** page, enter a description of the data source in the **Computer Description** field.
4. In the **Computer Name** field, enter the IP address or fully qualified domain name (FQDN) for the data source.
5. From the **Computer Type** drop-down menu, select **Microsoft Windows**, and turn on **Enable File Share Backups**.
6. Specify the file share credentials in the **Microsoft Windows Computer Information** section, and then click **Test Credentials**.
7. Click **Save** at the top of the page; the **Add Data Source** page displays.
8. In the **Backup** section, in the **Data Description** field, enter a label for the data source you are backing up.
9. From the **Data Type** drop-down menu, select **File Share - CIFS**.
10. In the **File Share Information** section, enter the exact name of the network share on the server, for example, **`C$`**, needed to access the data source from devices on the local network, and then click **Test Share** to test Share connectivity.
11. If you wish to view all available network shares on the server, click **Toggle All Shares**, and then click **Fetch Data Sources** to automatically populate the list of data sources.
12. In the **Folder Selection** section, you can select all folders in the network share, or optionally select specific folders you wish to back up:



Data Description: C$ - Docs and Settings

Describe the data source you are backing up.

Select to back up this data source on the configured backup schedule. If this is unchecked, then the backup schedule will not apply to this data source.

☑ Enable Backups

The name of the Network Share. For SSHFS connections (Mac OS X/Linux/Unix), enter the full path to the directory being backed up. *Test Share* verifies open connectivity between the target and backup servers.

Share Name: C$

Status: Successfully connected to computer.

Select All Folders will back up everything within the data source. *Pick Certain Folders* allows you to specify folders within the data source. *Fetch Folders* refreshes the folder list.

○ Select All Folders

● Pick Certain Folders

Notice: Folders that are *not* selected will not be backed up. Deselecting a folder will cause data to be purged from the backup server after 24 hours.

Folders:

- ☐ $Recycle.Bin
- ☐ Boot
- ☑ Documents and Settings
- ☐ ExchangeSetupLogs
- ☐ PerfLogs
- ☐ Program Files
- ☐ Program Files (x86)
- ☐ ProgramData
- ☐ RestoreData
- ☐ System Volume Information
- ☑ Users

13. To replicate to the cloud, turn on **Replicate to Barracuda Cloud Storage**; note that if you have globally selected to replicate to the cloud, you cannot change this setting.

> **Replication**
> If you wish to set up replication to another Barracuda Backup Server, turn on **Replicate to Other Barracuda Backup Servers**, and click **Add a new Backup Server**. For detailed steps, refer to Configuring a Replication Destination.

14. Click **Save** at the top of the page.

Create Backup Schedules

> A schedule is automatically created (with the default set to back up every day at 8:00PM) when a data source is created *except* if a schedule specifying *all* data sources already exists.

To create a backup schedule, go to the **BACKUP > Schedules** page of the Barracuda Backup web interface. Click **Add a Schedule** and fill in the information on the **Add Backup Schedule** page.

Create Data Retention Policies

To set retention policies,

1. Go to the **BACKUP > Retention Policies** page, click **Add a Retention Policy**, and enter a name to identify the policy.
2. In the **Items to Retain** section, select the NAS data source to which the retention policy applies; the **Retention Timeline** section displays. Select a timeline template on which to base your retention policy, or specify your own revision timeline.
3. Select the desired **Removed Files Rule** setting, and click **Save**.

Configure Optional Features

You can optionally configure the following settings for the NAS data sources:

- **Back Up Rate Limit** - Rate limits control the data replication rate to Barracuda Cloud Storage or other offsite storage locations. You can limit Internet bandwidth consumption during peak usage times, and schedule backups for non-peak hours on the **BACKUP > Rate Limit** page.
- **Exclude Files from Backup** - You can create exclusion rules that use pattern matching to identify directory or file names that you do not wish to back up on the **BACKUP > Exclusions** page.

How to Back Up FirstClass Mail

> This article refers to firmware version 5.3 and higher, and the FirstClass Mail client running on Windows® or Linux/Unix.

In this article:

- Install the Agent
- Replicate Data
- Add FirstClass Mail as a Data Source

Related Articles
Creating Backup Schedules Setting Up Exclusion Rules Creating Retention Policies

Install the Agent

Use the following steps to install the Barracuda Backup Agent:

1. Log in to the Barracuda Backup web interface, and selected the associated Barracuda Backup Server in the left pane.
2. Go to the **SYSTEM > Software Downloads** page, and select the appropriate Agent for the environment in which you are running FirstClass Mail:
    - If you are running FirstClass in Windows, download and install the Barracuda Backup Agent (Windows).
    - If you are running FirstClass in a Linux/Unix environment, download and unzip the Barracuda Backup Agent

(Linux) on your local Linux system or server.

Replicate Data

If you are replicating data to another FirstClass Mail Server, you must disable mirroring when backups run.

You can run pre- and post commands to stop and start this process.

> **Permissions**
> To run these commands you must have permissions to the FCP utility fcputility.

To pause mirroring, use the command:

```
fcputil pause
```

To restart mirroring, use the command:

```
fcputil continue
```

> If the installed Agent has access to fcputility, you can run these commands from the Agent. For more information, refer to How to Create a Pre- or Post-Agent Backup Command Batch File or Script.

Add FirstClass Mail as a Data Source

Use the following steps to add FirstClass Mail as a data source:

1. Log in to the Barracuda Backup web interface, and selected the associated Barracuda Backup Server in the left pane.
2. Go to the **BACKUP > Sources** page, and click **Add Computer**.
3. Enter the FirstClass Network Store (FCNS) computer description, and enter the IP address or FQDN in the **Computer Name** field.
4. From the **Computer Type** drop-down menu, select either **Microsoft Windows** or **Linux / Unix**, and click **Save**.
5. In the **Add Data Source** page, select **Barracuda Agent Software** as the **Data Type**.
6. Click **Test Software Connectivity** to verify Barracuda Backup can communicate with the Agent.
7. In the **Item Selection** section, click **Select All Items** to back up the entire FCNS folder including desktop folders, calendar, contacts, etc., or click **Select Specific Items** to select individual items for backup.
8. Click **Save** at the top of the page.

FirstClass Mail backups will run at the next scheduled time.

How to Back Up NFS Mounts with the Barracuda Backup Agent (Linux)

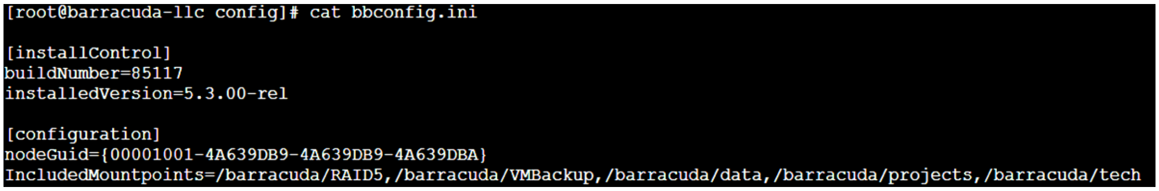
> This article refers to Barracuda Backup firmware version 5.3 and higher, and the Barracuda Backup Agent (Linux).

Back up NFS mounts using the Barracuda Linux Backup Agent.

Configure the Agent

Use the following steps to configure the Barracuda Backup Agent (Linux):

1. Log in to your Linux Server, and enter the following command to stop the Agent:
   ```
   # /etc/init.d/bbagent stop
   ```
2. Navigate to the Barracuda Backup Agent installation directory. The default location is: **/usr/local/barracuda/bbs/**
3. Open the **config** directory, and open the **bbconfig.ini** file in a text editor.
4. Below the **[configuration]** section, enter:
   ```
   IncludedMountpoints=/mount/mountpoint,/mount/mountpoint2
   ```
   For example:



```
[root@barracuda-llc config]# cat bbconfig.ini

[installControl]
buildNumber=85117
installedVersion=5.3.00-rel

[configuration]
nodeGuid={00001001-4A639DB9-4A639DB9-4A639DBA}
IncludedMountpoints=/barracuda/RAID5,/barracuda/VMBackup,/barracuda/data,/barracuda/projects,/barracuda/tech
```

5. Save and close the file.
6. Enter the following command to restart the Agent:
   `# /etc/init.d/bbagent start`

How to Back Up NSS Mounts with the Barracuda Backup Agent (Linux)

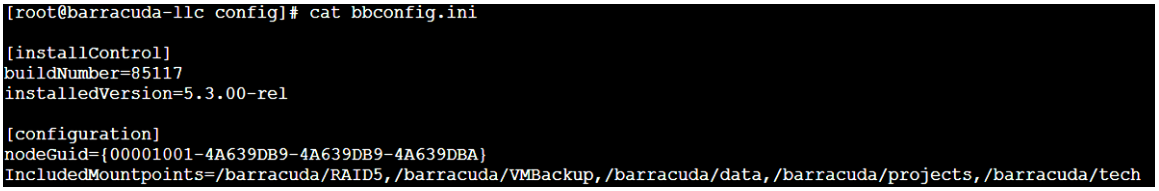
> This article refers to Barracuda Backup firmware version 5.3 and higher, the Barracuda Backup Agent (Linux) , and the Novell Storage Services (NSS) file system.

Back up NSS mounts using the Barracuda Backup Agent (Linux).

Configure the Agent

Use the following steps to configure the Barracuda Backup Agent (Linux):

1. Log in to your Linux Server, and enter the following command to stop the Agent:
   `# /etc/init.d/bbagent stop`
2. Navigate to the Barracuda Backup Agent installation directory. The default location is:
   /usr/local/barracuda/bbs/
3. Open the **config** directory, and open the **bbconfig.ini** file in a text editor.
4. Below the **[configuration]** section, enter:
   `IncludedMountpoints=`*`/mount/mountpoint,/mount/mountpoint2`*
   For example:



```
[root@barracuda-llc config]# cat bbconfig.ini

[installControl]
buildNumber=85117
installedVersion=5.3.00-rel

[configuration]
nodeGuid={00001001-4A639DB9-4A639DB9-4A639DBA}
IncludedMountpoints=/barracuda/RAID5,/barracuda/VMBackup,/barracuda/data,/barracuda/projects,/barracuda/tech
```

5. Save and close the file.
6. Enter the following command to restart the Agent:
   `# /etc/init.d/bbagent start`

Replication Page

> This article refers to Barracuda Backup firmware version 5.0 and higher.

Related Articles

- Configuring a Replication Destination
- Temporarily Disabling a Destination
- How to Manage the Data Queue
- Why Data is not Replicating to an Offsite Location

Barracuda Backup Servers that are used to back up data from one or more Barracuda Backup Servers are known as *destinations*. Data from one Barracuda Backup Server can be replicated to one or more destinations.

Backup Data Replication Configuration

Configure backup data replication to one or more other Barracuda Backup Servers. On the **BACKUP > Replication** page you can view:

- **Target List** - Displays where data *from* the selected Barracuda Backup Server is sent
- **Source List** - Displays a list of devices sending data *to* the selected Barracuda backup Server

A Barracuda Backup Server can act as a backup to one or more other Barracuda Backup Servers. Each Barracuda Backup Server can send data to one or more other Barracuda Backup Servers.

Important

- Only the Barracuda Backup Server 490 and higher can act as a backup to other Barracuda Backup Servers, although any Barracuda Backup Server can *send* data.
- Data can be backed up to both a second Barracuda Backup Server and to Barracuda Cloud Storage. Data that is backed up on a second Barracuda Backup Server *cannot* be backed up yet again onto another Barracuda Backup Server.
- For every Terabyte of data replicated, Barracuda Networks recommends a 1.5 Mbps or T1 connection.
- You must have the serial number and replication code of the destination. These can be found by selecting the destination Barracuda Backup Server and looking at its **BACKUP > Replication** page.

Before Getting Started

Before getting started, verify the following:

- Make sure that your retention policies are configured before configuring replication. Otherwise you may waste bandwidth copying data that does not need to be replicated.
- Verify Internet connectivity between the local and remote Barracuda Backup Server(s). Configuring a secure VPN connection between multiple Barracuda Backup Servers ensures the highest level of security possible.
- You must have the serial number and replication code of the *destination* Barracuda Backup Server. Go to the *destination* Barracuda Backup Server, and go to the **BACKUP > Replication** page. The serial number and replication code display at the top right of the page.

Continue with Configure a Replication Destination.

Configuring a Replication Destination

This article refers to Barracuda Backup firmware version 4.2 or higher.

In this article:

- Edit Replication Server Settings
- Remove a Barracuda Backup Server
- Send Data To/Receiving Data From

Related Articles

- Configuring Replication
- How to Restore from a Replication Destination
- How to Temporarily Disable a Destination
- Why Data is not Replicating to an Offsite Location

Important

- Only the Barracuda Backup Server 490 and higher can act as a backup to other Barracuda Backup Servers, although any Barracuda Backup Server can *send* data.
- Data can be backed up to both a second Barracuda Backup Server and to Barracuda Cloud Storage. Data that is backed up on a second Barracuda Backup Server *cannot* be backed up yet again onto another Barracuda Backup Server.
- For every Terabyte of data replicated, Barracuda Networks recommends a 1.5 Mbps or T1 connection.
- You must have the serial number and replication code of the destination. These can be found by selecting the destination Barracuda Backup Server and looking at its **BACKUP > Replication** page.

Barracuda Backup Servers that are used to back up the data from one or more Barracuda Backup Servers are known as destinations. Data from one Barracuda Backup Server can be replicated to one or more destinations.

To configure where data is replicated to from a Barracuda Backup Server,

1. Select the Barracuda Backup Server in the list to which you wish to *add* a replication destination, and go to the **BACKUP > Replication** page.
2. To add a replication destination, click **Add a Target**.
3. In the **Add Destination** page, select from one of the following options:
    - From the **Backup Server** list, select a Barracuda Backup Server from your account to automatically load the required destination details, *or*
    - Enter the following details in the associated fields:
        - Enter the destination hostname or IP address
        - Enter the Serial Number from the *destination* Barracuda Backup Server
        - Enter the Replication Code from the *destination* Barracuda Backup Server
4. Click **Save**.

Once a destination is added, it appears in the **Sending Data To** table. If the status displays as online (Online ●), the two systems are able to communicate with each other.

On the **BACKUP > Replication** page, there is a global flag to replicate all data to either Barracuda Cloud Storage or to Barracuda Backup Servers:

☑ Send All Local Backups ●

If you wish to send data from diverse sources to both of these options, then *do not* set this flag on any items in the Target List. Instead, edit each data source on the **BACKUP > Sources** page, and specify where its data is to be replicated.

Edit Replication Server Settings

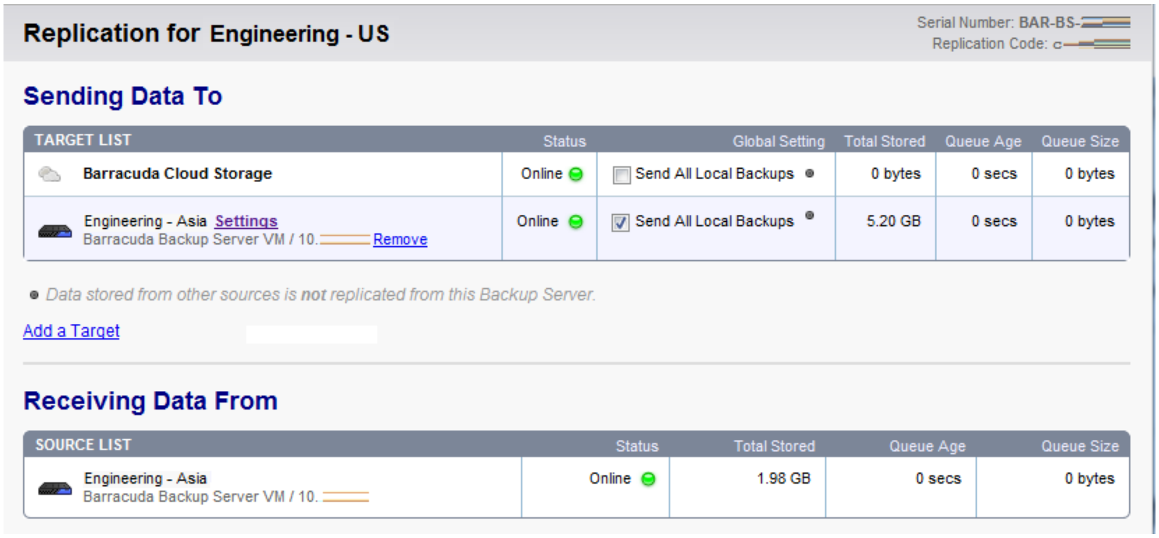
To edit the replication target settings, click **Settings** in the **Target List**. In the **Replication Target Settings** list, you can modify the destination IP address, disable data replication, and specify whether to send all data on the Barracuda Backup Server to this target.

Remove a Barracuda Backup Server

To permanently remove a replication destination, click **Remove** in the **Target List**.

Send Data To/Receiving Data From

Destination Barracuda Backup Servers display in the **Sending Data To** table. If a Barracuda Backup Server is acting as a destination for another Barracuda Backup Server, it displays in the **Receiving Data From** table.



Replication for Engineering - US

Serial Number: BAR-BS-[redacted]
Replication Code: c[redacted]

Sending Data To

TARGET LIST	Status	Global Setting	Total Stored	Queue Age	Queue Size
Barracuda Cloud Storage	Online ●	☐ Send All Local Backups ●	0 bytes	0 secs	0 bytes
Engineering - Asia Settings Barracuda Backup Server VM / 10.[redacted] Remove	Online ●	☑ Send All Local Backups ●	5.20 GB	0 secs	0 bytes

● *Data stored from other sources is **not** replicated from this Backup Server.*

Add a Target

Receiving Data From

SOURCE LIST	Status	Total Stored	Queue Age	Queue Size
Engineering - Asia Barracuda Backup Server VM / 10.[redacted]	Online ●	1.98 GB	0 secs	0 bytes

How to Temporarily Disable a Destination

You can temporarily disable the site-to-site replication feature for one or more destinations. If it is disabled, nothing is sent from the Barracuda Backup Server to the destination until the feature is enabled or until 24 hours have passed. This allows you to move the destination system to a remote location, say, without getting backup errors. If the 24 hours pass without a manual re-enabling of this feature, the Barracuda Backup Servers attempt to communicate with each other and, if successful, perform the backups.

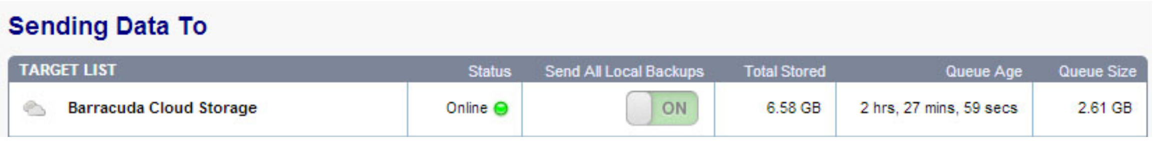
To temporarily disable site-to-site replication, go to the **BACKUP > Replication** page. In the **Sending Data To** table, click on the **Settings** link beside the destination Barracuda Backup Server. On the **Replication Target Settings** page there is a setting to disable data replication for up to 24 hours.

How to Manage the Data Queue

If there is a loss of communication between the Barracuda Backup Server and its back up destination for any reason, the data to be backed up is queued and errors generated. Data is queued until the issue is resolved. The queue size in the table on the **BACKUP > Replication** page indicates how much data is waiting to be replicated.

> Note that not all of this data is actually copied to the destination. Some of it is deduplicated as the replication proceeds. Only those parts that are not already stored in the remote location are sent over the Internet.

The following queue details display on the **BACKUP > Replication** page:



Sending Data To

TARGET LIST	Status	Send All Local Backups	Total Stored	Queue Age	Queue Size
Barracuda Cloud Storage	Online ●	ON	6.58 GB	2 hrs, 27 mins, 59 secs	2.61 GB

- **Status** - Displays either the green indicator (Online ●) icon or the red indicator (Offline ■) icon
- **Total Stored** - Total size of file parts transferred offsite from the Barracuda Backup Server
- **Queue Age** - Amount of time that the queued data has been waiting to be transferred offsite from the Barracuda Backup Server
- **Queue Size** - Total size of the file parts yet to be transferred offsite from the Barracuda Backup Server

Schedules Page

This article refers to Barracuda Backup firmware version 5.0 and higher.

In this article:

- Data Backup
- Adding a Schedule
- Schedule Options

Once you configure computers and data sources, create backup schedules, either individually or for all sources.

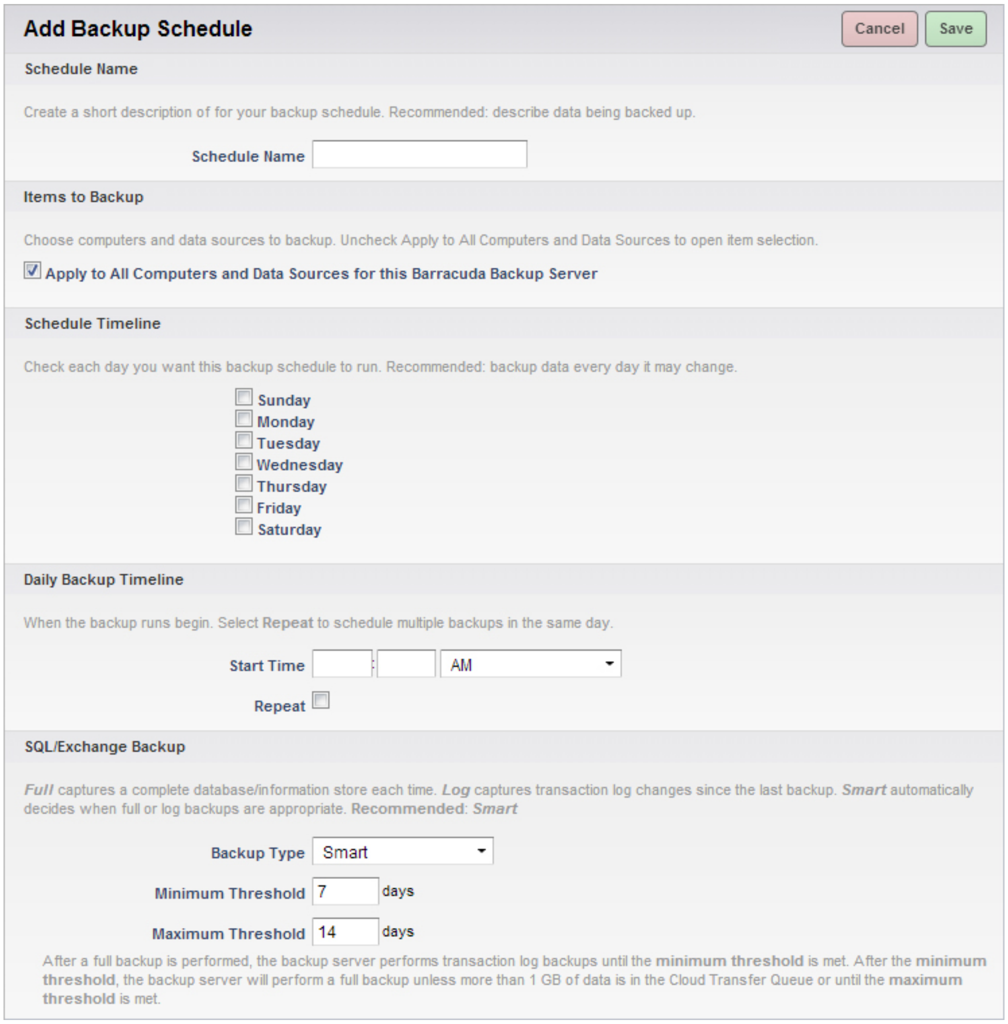
If no schedule is created for a data source then it will not be backed up. Data sources that do not have a schedule applied display at the top of the page in a yellow note box.

Data Backup

Once your Barracuda Backup Server is installed and data sources are set up, data is collected from each data source for the first time during an initial backup period. Once the initial backup is complete, Barracuda Backup checks for changed and new data based on backup schedules you define on the **BACKUP > Schedules** page. Any data sources that do not have a schedule defined are, by default, backed up nightly at 8:00PM local time. When Barracuda Backup identifies new or changed information, each file is analyzed at the bit level, and only the new bit sequences in the files themselves are copied and transferred, saving both bandwidth and storage space.

Adding a Schedule

To create a backup schedule, go to the **BACKUP > Schedules** page of the Barracuda Backup web interface. Click **Add a Schedule** and fill in the information on the **Add Backup Schedule** page:



Add Backup Schedule

Schedule Name

Create a short description of for your backup schedule. Recommended: describe data being backed up.

Schedule Name ☐

Items to Backup

Choose computers and data sources to backup. Uncheck Apply to All Computers and Data Sources to open item selection.

☑ Apply to All Computers and Data Sources for this Barracuda Backup Server

Schedule Timeline

Check each day you want this backup schedule to run. Recommended: backup data every day it may change.

- ☐ Sunday
- ☐ Monday
- ☐ Tuesday
- ☐ Wednesday
- ☐ Thursday
- ☐ Friday
- ☐ Saturday

Daily Backup Timeline

When the backup runs begin. Select **Repeat** to schedule multiple backups in the same day.

Start Time : AM

Repeat ☐

SQL/Exchange Backup

Full captures a complete database/information store each time. ***Log*** captures transaction log changes since the last backup. ***Smart*** automatically decides when full or log backups are appropriate. **Recommended: *Smart***

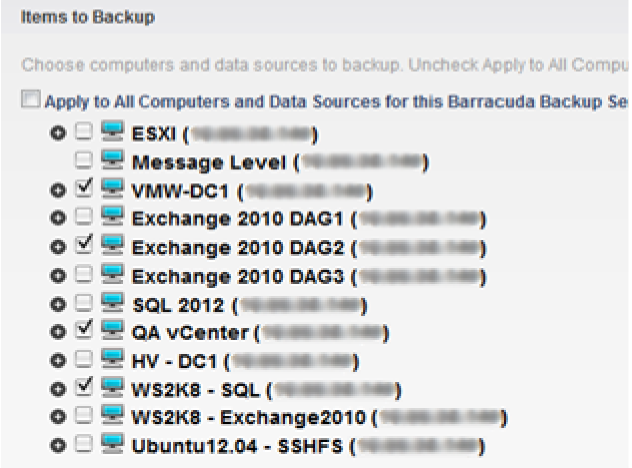
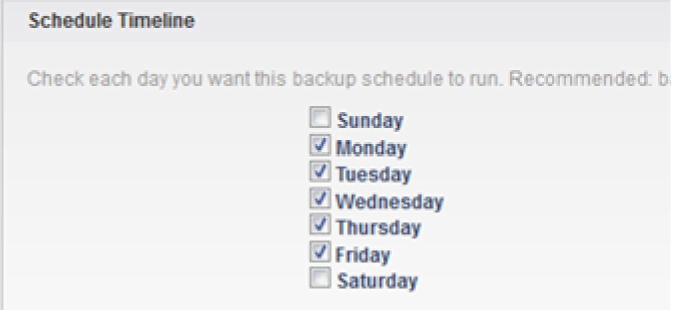
Backup Type Smart

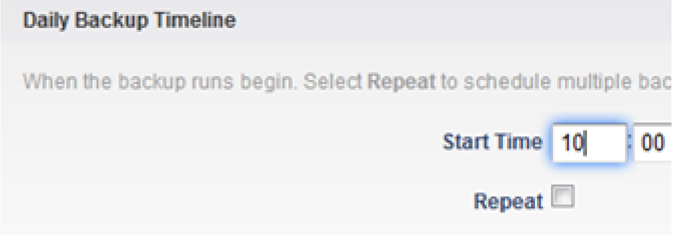
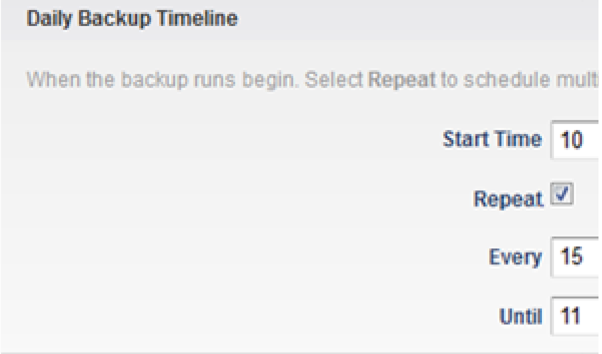
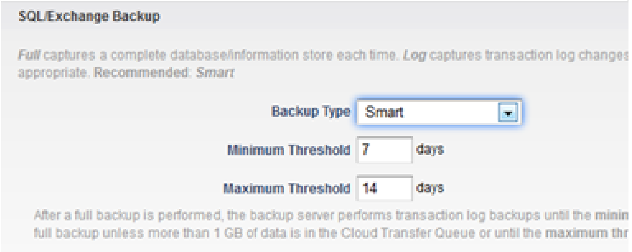
Minimum Threshold 7 days

Maximum Threshold 14 days

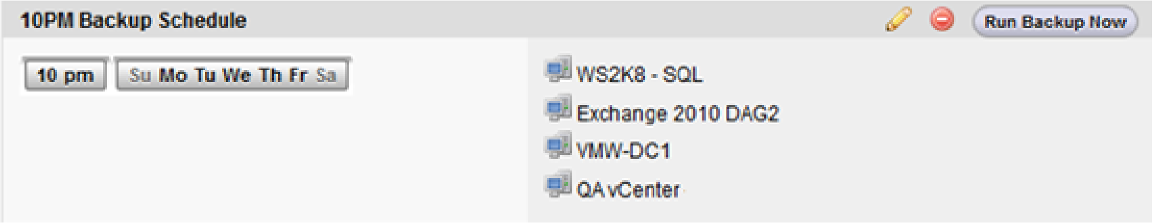
After a full backup is performed, the backup server performs transaction log backups until the **minimum threshold** is met. After the **minimum threshold**, the backup server will perform a full backup unless more than 1 GB of data is in the Cloud Transfer Queue or until the **maximum threshold** is met.

Field	Description
Schedule Name	Enter a label to identify the backup schedule.

Items to Back Up	- Turn on **Apply to All Computers and Data Sources for this Barracuda Backup Server** to apply this schedule to all content - Turn off **Apply to All Computers and Data Sources for this Barracuda Backup Server** and expand and select specific items to apply this schedule to a specific data source or group of data sources:  Items to Backup Choose computers and data sources to backup. Uncheck Apply to All Compu ☐ Apply to All Computers and Data Sources for this Barracuda Backup Se ☐ ESXI ([redacted]) ☐ Message Level ([redacted]) ☑ VMW-DC1 ([redacted]) ☐ Exchange 2010 DAG1 ([redacted]) ☑ Exchange 2010 DAG2 ([redacted]) ☐ Exchange 2010 DAG3 ([redacted]) ☐ SQL 2012 ([redacted]) ☑ QA vCenter ([redacted]) ☐ HV - DC1 ([redacted]) ☑ WS2K8 - SQL ([redacted]) ☐ WS2K8 - Exchange2010 ([redacted]) ☐ Ubuntu12.04 - SSHFS ([redacted])
Schedule Timeline	Turn on the days on which to run the backup:  Schedule Timeline Check each day you want this backup schedule to run. Recommended: b ☐ Sunday ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☐ Saturday

Daily Backup Timeline	Enter the start time; turn on **Repeat** if you wish to specify a time period and end date to repeat the backup:  Daily Backup Timeline When the backup runs begin. Select **Repeat** to schedule multiple bac Start Time 10 : 00 Repeat ☐ **Multiple Daily Backups** If you turn on **Repeat**, you can run multiple backups daily. For example, in the following image, the back up start time is 10:00PM, and the backup schedule will repeat at 10:15PM, 10:30PM, 10:45PM, and so on until stopping at the time in the **Until** field:  Daily Backup Timeline When the backup runs begin. Select **Repeat** to schedule mult Start Time 10 Repeat ☑ Every 15 Until 11 This schedule only applies to the current day, so you cannot start a backup at night and then repeat it until the next morning. Instead, create a separate schedule after midnight or start the original backup job in the morning and repeat it throughout the day.
SQL/Exchange Backup	If the backup schedule is for Microsoft$^{®}$ SQL Server$^{®}$ or Microsoft Exchange Server, you must specify the type of backup to run: • **Smart** - After a full backup is performed, the backup server performs transaction log backups until the **minimum threshold** is met. After the **minimum threshold** is met, the Barracuda Backup Server performs a full backup unless there is more than 1 GB of data in the Cloud Transfer Queue, or until the **maximum threshold** is met. • **Full** - A **Full Backup** captures a complete database/information store each time. • **Log** - A **Log Backup** captures transaction log changes since the last backup.  SQL/Exchange Backup *Full* captures a complete database/information store each time. *Log* captures transaction log changes appropriate. Recommended: *Smart* Backup Type Smart Minimum Threshold 7 days Maximum Threshold 14 days After a full backup is performed, the backup server performs transaction log backups until the **minin** full backup unless more than 1 GB of data is in the Cloud Transfer Queue or until the **maximum thr**

Once you are satisfied with your new schedule, click **Save**. The new schedule displays on the **BACKUP > Schedules** page:



10PM Backup Schedule

Run Backup Now

10 pm | Su Mo Tu We Th Fr Sa

WS2K8 - SQL
Exchange 2010 DAG2
VMW-DC1
QA vCenter

Schedule Options

Once you create a backup schedule, you can edit, delete, or immediately run a backup:

- **Edit Schedule** (✎) icon - Click to access the **Edit Backup Schedule** page. Make the desired modifications to the schedule, and then click **Save** at the top of the page.
- **Remove Schedule** (⊖) icon - Click to delete the selected schedule, and click **Remove Schedule** in the dialog box to verify you wish to remove the selected schedule.
- **Run Backup Now** (Run Backup Now) icon - Click to run the scheduled backup process immediately, and click **Run Backup Now** in the dialog box that follows to verify your the selected action. Once the backup starts, allow a few minutes for the report to generate on the **REPORTS > Backup** page.

Rate Limit Page

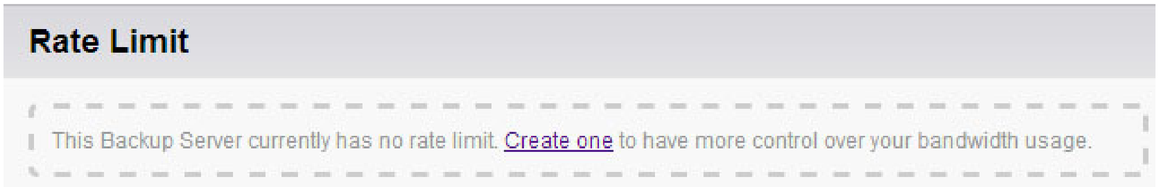
This article applies to Barracuda Backup firmware version 5.0 and higher.

Rate limits control the data replication rate to Barracuda Cloud Storage or other offsite storage locations. You can limit Internet bandwidth consumption during peak usage times, and schedule backups for non-peak hours.

Your initial offsite backup may take on the order of days to complete but all of the data is backed up locally on the Barracuda Backup Server during this period. After the initial large transfer is complete, replicating your data offsite should complete with only a few hours of transfer each day. By default, Barracuda Backup is configured to run full speed data transfers at night so that bandwidth is not affected while most people are at work. An alternate rate limit allows you to adjust the limit speed and time interval.

The length of transfer time it will take to get your data offsite is impacted by the compression and deduplication rates on your data, the uplink speed of your Internet connection, the amount of data that changes every day, and any speed limits you apply to Barracuda Backup.

If you do not set a rate limit, the **BACKUP > Rate Limit** page displays the following message:

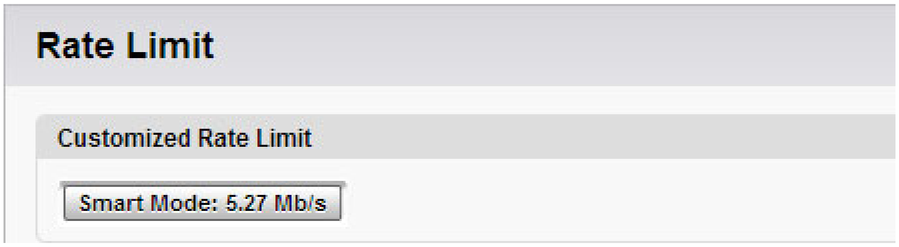


Rate Limit

This Backup Server currently has no rate limit. Create one to have more control over your bandwidth usage.

Click **Create one** to set up a rate limit.

Once you create a rate limit, the **BACKUP > Rate Limit** page displays the customized rate limit settings:



Rate Limit

Customized Rate Limit

Smart Mode: 5.27 Mb/s

If you have created a rate limit, you can take the following actions on the **BACKUP > Rate Limit** page:

- **Edit Rate Limit** (✎) icon - Click to edit the rate limit. Select from the options listed in the following table:

Option	Settings	Details
Default Rate Limit	• **Full Speed** - Uses 100% of available bandwidth • **Smart Mode** - Drag the **Percent of Bandwidth** bar to specify the rate limit; click **Test bandwidth** to verify your setting • **Kb/s or Mb/s** - Specify the rate limit in Kilobits or Megabits per second	Specify the default rate limit.
Alternate Rate Limit	• **Full Speed -** Uses 100% of available bandwidth • **Smart Mode** - Drag the **Percent of Bandwidth** bar to specify the rate limit; click **Test bandwidth** to verify your setting • **Kb/s or Mb/s** - Specify the rate limit in Kilobits or Megabits per second	You can optionally create an alternate rate limit which is maintained only during the specified time periods: • **From/To -** Specify the start and end time • **On -** Select the days to which the alternate rate limit applies.

- **Reset to Default Rate Limit** (↩) icon - Click to rest the selected Barracuda Backup Server to the default rate limit; click **Reset To Defaults** in the dialog box that follows to complete your selection.

Exclusions Page

This article applies to Barracuda Backup firmware version 5.0 and higher.

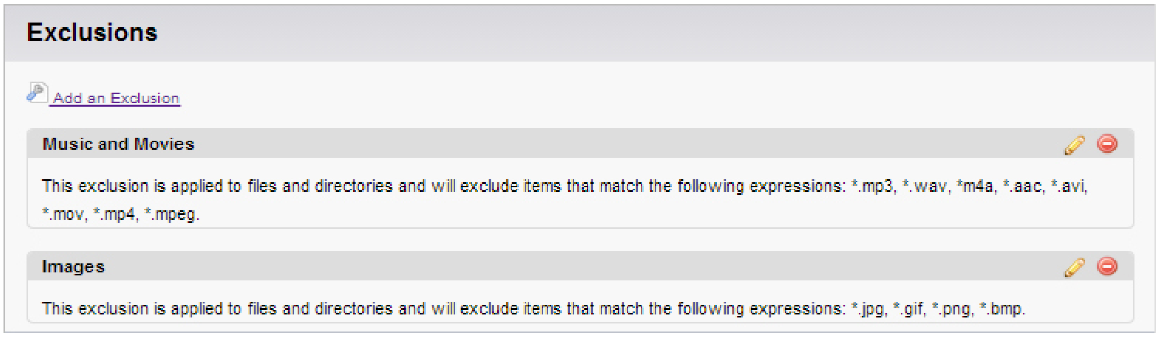
You can create exclusion rules that use pattern matching to identify directory or file names that are not to be backed up. Files which are typically excluded from backups include temporary files, music, movies and other files which are not essential for business needs.

Use the following steps to create an exclusion rule:

1. Log in to the Barracuda Backup web interface, and select the associated Barracuda Backup Server in the left pane.
2. Go to the **BACKUP > Exclusions** page, and click **Add an Exclusion**.
3. Fill in the information on the **Add an Exclusion** page:
    - **Exclusion Rule Name** - Enter a descriptive label to identify the exclusion rule.
    - **Add Exclusions to Reports** - Specify whether to include exclusions in reports.
    - **Apply Recursively to Sub Directories** - Specify whether to apply the exclusion rule recursively to sub directories.
    - **Where to Exclude** - Specify whether to apply the exclusion rule to all computers and data sources for the selected Barracuda Backup Server.
4. In the **What to Exclude** section, specify the excluded file types:
    - From the **Preset Expressions** menu, select the content you want to exclude, for example, **Audio files**, then click **Add**.
    - In the **Expressions** field, enter a search string to exclude, for example, ***.mp3**, then click **Add**.

    Use Case
    For example, a school organization does not want to back up music files located in user home directories. To exclude these music files, they create an exclusion rule, select the directory, select the preset expression **Audio files**, and enter the types of music files they want to exclude in the **Expressions** field.

5. click **Save** at the top of the page to add the exclusion rule.



Exclusions

Add an Exclusion

Music and Movies

This exclusion is applied to files and directories and will exclude items that match the following expressions: *.mp3, *.wav, *m4a, *.aac, *.avi, *.mov, *.mp4, *.mpeg.

Images

This exclusion is applied to files and directories and will exclude items that match the following expressions: *.jpg, *.gif, *.png, *.bmp.

To edit an existing exclusion rule, go to the **BACKUP > Exclusions** page of the Barracuda Backup web interface, and click the **Edit Exclusion** (✎) icon following the exclusion rule you want to edit. Make the desired changes, then click **Save**.

To delete an exclusion rule, go to the **BACKUP > Exclusions** page of the Barracuda Backup web interface, and click the **Remove Exclusion** (⊖) icon following the exclusion rule you want to remove. Click **OK** to confirm you want to remove the rule.

Retention Policies Page

Related Articles
- Understanding Retention Policies - How to Create Retention Policies - Understanding Barracuda Offsite Vaulting - Creating Effective Retention Policies - Retention Policy Example

Configure retention policies for data stored on a Barracuda Backup Server on the **BACKUP > Retention Policies** page. Be sure to configure retention policies for your data. Not doing so means that some unwanted data will be moved across the Internet and stored, causing unnecessary expense.

Data is retained based on a traditional grandfather-father-son (daily-weekly-monthly) rotation model. You can specify how long to keep daily, weekly, monthly, and yearly backups by creating data retention policies. Multiple retention policies can be created for files, data backed up by the Barracuda Backup Agent (Exchange, SQL, System State), and email messages.

There are some template policies provided to assist you in creating your own retention policies. You can create one policy for all data sources on a Barracuda Backup Server or multiple policies that each include some subset of the data.

When data is removed according to a retention policy, it is deleted from both the local Barracuda Backup Server and the offsite storage locations. Removed files that have been backed up using Network File Shares Protocol or SSHFS may be retained for a longer period of time, according to the configuration. Otherwise, once your data has been purged, it is gone forever. Purging applies to historic file revisions only; your current data is not impacted by a retention policy. If you wish to purge data immediately for a specific retention policy, go to the **BACKUP > Retention Policies** page, and click the **Start Purge Process** (Start Purge Process) icon, and click **Start Purge Process** in the dialog that follows to confirm your selection.

> ⚠ Purging applies to *historic file revisions only;* your current data is never impacted by a retention policy.

Understanding Retention Policies

Related Articles
- How to Create Retention Policies - Creating Effective Retention Policies - Retention Policy Example - Offsite Vaulting (firmware version 5.4 and higher only)

Use retention policies to define the length of time you retain historic data based on daily, weekly, monthly, or yearly time intervals. Barracuda

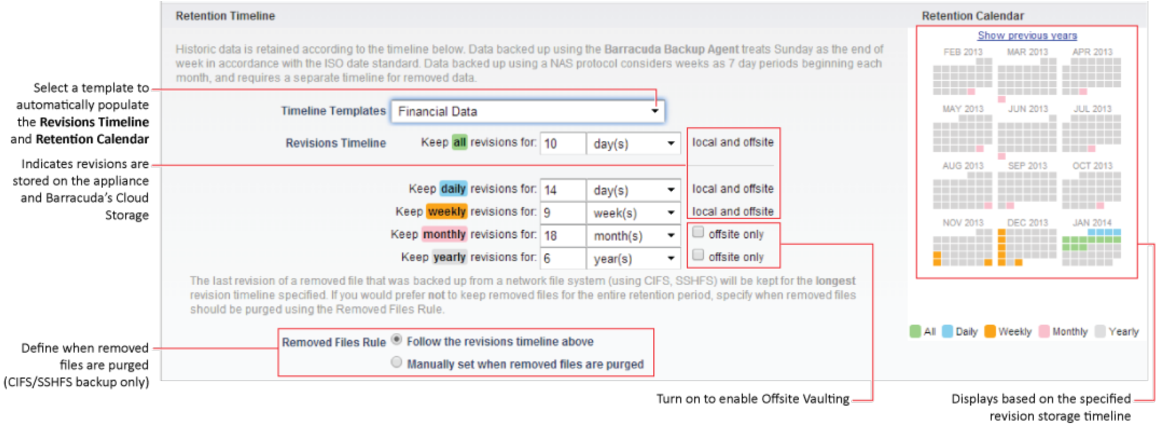
Backup retention policies can be created for different sets of data including virtual machines, data backed up by the Barracuda Backup Agent (Exchange, SQL, Hyper-V, System State), and email messages. You can create one policy for all of the computers and data sources on Barracuda Backup or create multiple policies for each data source. Use the **BACKUP > Retention Policy** page to define content retention rules:

- **Policy Name** - Enter an identifying name for the policy
- **Items to Retain** - Displays all data sources on the selected Barracuda Backup Server. Select all of the items you want to include in the retention policy.

> Items with no retention policy are retained forever on the local appliance.

- **Retention Timeline** - Define how historic data is retained.

> Data backed up using the Barracuda Backup Agent treats Sunday as the end of week in accordance with the ISO date standard. Data backed up using a NAS protocol considers weeks as seven day periods beginning each month.


Select a template to automatically populate the **Revisions Timeline** and **Retention Calendar**
Indicates revisions are stored on the appliance and Barracuda's Cloud Storage
Define when removed files are purged (CIFS/SSHFS backup only)
Turn on to enable Offsite Vaulting
Displays based on the specified revision storage timeline
Show previous years
FEB 2013
MAR 2013
APR 2013
MAY 2013
JUN 2013
JUL 2013
AUG 2013
SEP 2013
OCT 2013
NOV 2013
DEC 2013
JAN 2014
🟩 All
🟦 Daily
🟧 Weekly
🟥 Monthly
⬜ Yearly

Retention Timeline

Historic data is retained according to the timeline below. Data backed up using the **Barracuda Backup Agent** treats Sunday as the end of week in accordance with the ISO date standard. Data backed up using a NAS protocol considers weeks as 7 day periods beginning each month, and requires a separate timeline for removed data.

Timeline Templates: Financial Data

Revisions Timeline
Keep **all** revisions for: 10 day(s) local and offsite
Keep **daily** revisions for: 14 day(s) local and offsite
Keep **weekly** revisions for: 9 week(s) local and offsite
Keep **monthly** revisions for: 18 month(s) ☐ offsite only
Keep **yearly** revisions for: 6 year(s) ☐ offsite only

The last revision of a removed file that was backed up from a network file system (using CIFS, SSHFS) will be kept for the **longest** revision timeline specified. If you would prefer **not** to keep removed files for the entire retention period, specify when removed files should be purged using the Removed Files Rule.

Removed Files Rule
● Follow the revisions timeline above
○ Manually set when removed files are purged

Retention Calendar

  - **Timeline Templates** - Select from the pre-defined templates which you can modify, or create your own custom timeline. The **Revisions Timeline** and **Retention Calendar** display the timeline based on the selected template.
  - **Revisions Timeline** - Define how long to keep daily, weekly, monthly, and yearly backups.

> **Local and Offsite Revision Storage**
> **Local and offsite** means that revisions are stored both on the physical Barracuda Backup appliance and in Barracuda's Cloud Storage or to another Barracuda Backup Server. Set this value based on your business requirements. Keeping revisions **forever** can affect your cloud storage requirements.

    - **Keep all revisions for** - Specify the number of **day(s)** to keep all content revisions, or select **never** or **forever**.

> This features allows you to keep revisions when you have multiple backups per day. For example, you back up your SQL Server hourly for 5 days giving you 120 revisions.

    - **Keep daily revisions for** - Specify how long to keep daily revisions. Specify a number of **day(s)**, **never**, or **forever**.
    - **Keep monthly revisions for** - Specify how long to keep weekly revisions. Specify a number of **week(s)**, **never**, or **forever**. Turn on **offsite only** to use Barracuda Offsite Vaulting.
    - **Keep yearly revisions for** - Specify how long to keep yearly revisions. Specify a number of **years(s)**, **never**, or **forever**. Turn on **offsite only** to use Barracuda Offsite Vaulting.

> **Offsite Vaulting**
> Offsite vaulting leverages Barracuda's replication technology to offload up to twelve monthly and seven yearly revisions to an offsite location, freeing up disk space on your local Barracuda Backup Server. This feature maintains your organization's compliance with long retention policies, allowing you to save more daily and weekly revisions. Note that offsite vaulting is available for both Barracuda Cloud and box-to-box replication. For more information, see Understanding Barracuda Offsite Vaulting.

        - **Retention Calendar** - Display the timeline based on the values in the **Revisions Timeline**. Click **Show previous years** to view prior year retention timelines.
- **Removed Files Rule** *(only applies to data backed up using file-based protocol (CIFS) or SSHFS)* - The last revision of a removed file that was backed up from a network file system (using CIFS, SSHFS) is kept for the *longest revision timeline specified*. If you would prefer not to keep removed files for the entire retention period, specify when removed files should be purged using the **Removed Files Rule**:
    - **Follow the revisions timeline above** - When selected, files are removed based on the **Revisions Timeline**.
    - **Manually set when removed files are purged** - When selected, you can specify the **Removed Files Timeline**:
        - **Removed Files Timeline** - Specify the number of **day(s)**, **week(s)**, **month(s)**, **years(s)**, **never**, or **forever** to keep removed files.

How to Create Retention Policies

This article refers to Barracuda Backup firmware version 4.3 and higher.

In this article:

- Create a Retention Policy
- Removed Files Rule
- Removed Email Timeline

Related Articles

- Understanding Retention Policies
- Creating Effective Retention Policies
- Retention Policy Example
- Offsite Vaulting (firmware version 5.4 and higher only)

Use retention policies to define the length of time you retain historic data based on daily, weekly, monthly, or annual time intervals. This allows you to manage data storage and growth.

⚠ **Important**
Purging applies to *historic file revisions only;* your current data is never impacted by a retention policy.

Create a Retention Policy

To set retention policies,

1. Go to the **BACKUP > Retention Policies** page, click **Add a Retention Policy**, and enter a name to identify the policy.
2. In the **Items to Retain** section, specify the data sources to which the retention policy applies; the **Retention Timeline** section displays. Select a timeline template on which to base your retention policy, or specify your own revision timeline.
3. Select the desired **Removed Files Rule** setting, and click **Save**.

Removed Files Rule

If you do not want to keep removed files for the entire retention period, specify when removed files should be purged using the **Removed Files Rule:**

- **Follow the revisions timeline above** (default) - Directs Barracuda Backup to follow the rules set in the **Revisions Timeline** section
- **Manually set when removed files are purged** - When selected, you specify the additional amount of times to keep removed files. You can specify in days, weeks, months, or years, or you can select **never** or **forever**

Removed Email Timeline

Specify how long to retain removed email messages. After the specified period of time, removed messages are purged. You can specify in days, weeks, months, or years, or select **never** or **forever**.

Understanding Barracuda Offsite Vaulting

This article refers to Barracuda Backup firmware version 5.4 or higher.

Related Articles

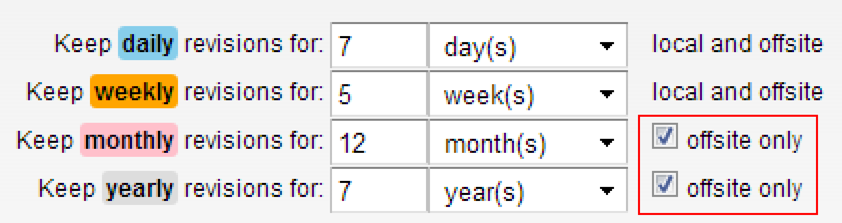
- Understanding Retention Policies
- How to Create Retention Policies
- Creating Effective Retention Policies

Offsite vaulting leverages Barracuda's replication technology to offload up to twelve monthly and seven yearly revisions to an offsite location, freeing up disk space on your local Barracuda Backup Server. This feature maintains your organization's compliance with long retention policies, allowing you to save more daily and weekly revisions. Note that offsite vaulting is available for both Barracuda Cloud and box-to-box replication. Offsite vaulting can be used for 12 monthly and 7 yearly historical revisions; these revisions are retained at the end of each calendar month and year.

⚠ **Warning**
Once offsite vaulting is enabled, it *cannot* be undone.

To specify offsite vaulting,

1. Log in to Barracuda Backup, and select the associated Barracuda Backup Server in the left pane.
2. Go to the **BACKUP > Retention Policies** page.
3. Click the **Edit Retention Policy** (✏) icon to the right of the retention policy you want to configure monthly and/or yearly offsite revisions.
4. Scroll down to the **Retention Timeline** section.
5. Select **offsite only** following **weekly** and/or **monthly**, and enter the associated time to keep the revisions:



Keep daily revisions for: 7 day(s) local and offsite
Keep weekly revisions for: 5 week(s) local and offsite
Keep monthly revisions for: 12 month(s) ☑ offsite only
Keep yearly revisions for: 7 year(s) ☑ offsite only

⚠ **Offsite Only**
Monthly and/or yearly revisions sent **offsite only** are purged from the local Barracuda Backup Server, and all revisions outside of this policy will be purged both locally and offsite.

6. Click the **Save** to apply your changes.

Creating Effective Retention Policies

This article refers to Barracuda Backup firmware version 4.3 and higher.

In this article:

- How it Works
- Revision Timelines
- Removed Files Rule
- Removed Email Timeline

Related Articles

- Understanding Retention Policies
- How to Create Retention Policies
- Retention Policy Example
- Understanding Barracuda Offsite Vaulting (firmware version 5.4 and higher only)

⚠ **Important**
Before defining data retention policies, make sure you have a clear understanding of data and email message compliance rules as well as your organization's record retention policies.

Use retention policies to define the length of time you retain historic data based on daily, weekly, monthly, or annual time intervals. This allows you to manage data storage and growth.

⚠ **Important**
Purging applies to *historic file revisions only;* your current data is never impacted by a retention policy.

Use the Barracuda Backup web interface to verify retention policies are in place and enforced. You can create different retention policies for different sets of data including:

- Files
- Data backed up by the Barracuda Backup Agent (Exchange, SQL, system state)
- Email messages

How it Works

Data is retained based on a traditional grandfather-father-son (daily-weekly-monthly) rotation model. You specify how long to keep daily, weekly, monthly, and yearly backups through data retention policies.

When you define a retention policy, begin by selecting either a preset template or a previously defined policy as a starting point. This helps you avoid creating multiple retention policies for the same sets of data. You can create one policy for all of the computers and data sources on a Barracuda Backup Server, or create different policies that include subsets of the data.

Revision Timelines

Historic data is retained based on your revision timeline settings.

Depending on how your data is backed up, revision timelines are treated in the following manner:

- Data backed up using the Barracuda Backup Agent treats Sunday as the end of week in accordance with the ISO date standard.
- Data backed up using a NAS protocol considers weeks as 7 day periods beginning each month, and requires a separate timeline for removed data.

Retention policies are based on retaining different types of data and different revisions for different periods of time. For example, in the General Documents Revision Template in the table below, all revisions are kept based on daily, weekly, and monthly revisions.

The predefined timeline templates use the revision timelines defined in the following table.

Revision Template	Keep All Revisions	Keep Daily Revisions	Keep Weekly Revisions	Keep Monthly Revisions	Keep Yearly Revisions
General Documents	5 days	1 week	1 month	1 year	never
Dump Files	Never	1 week	1 month	3 months	Never
Financial Data	10 days	2 weeks	2 months	18 months	6 years
Keep No Historic Data	Never	Never	Never	Never	Never
Exchange Data	Never	2 weeks	Never	Never	Never

SQL Server Database	Never	1 month	Never	Never	Never

Removed Files Rule

If you would prefer not to keep removed files for the entire retention period, you specify when removed files should be purged using the **Removed Files Rule:**

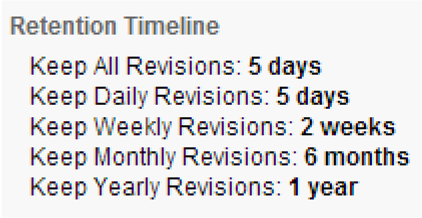
- **Follow the revisions timeline above** (default) - Directs Barracuda Backup to follow the rules set in the Revisions Timeline
- **Manually set when removed files are purged** - When selected, you specify the additional amount of times to keep removed files. You can specify in days, weeks, months, or years, or you can select **never** or **forever**

Removed Email Timeline

You can select how long to retain removed email messages. After the specified period of time, removed messages are purged. You can specify in days, weeks, months, or years, or select **never** or **forever**.

Retention Policy Example

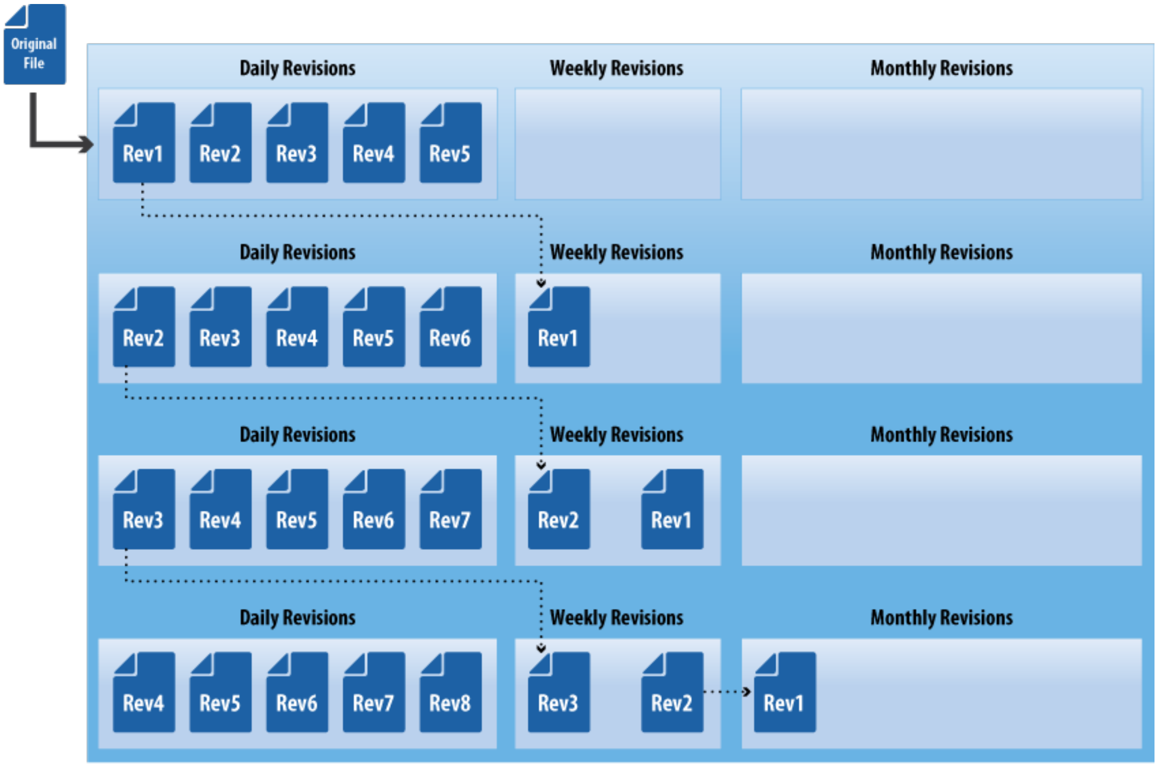
Use retention policies to define the length of time you retain historic data based on daily, weekly, monthly, or yearly time intervals. Think of retention policies in terms of your ability to restore data backed up in the past. For example, you have a retention timeline that keeps daily backups for five days, weekly backups for two weeks, monthly backups for six months, and yearly backups for one year:



Retention Timeline

Keep All Revisions: **5 days**
Keep Daily Revisions: **5 days**
Keep Weekly Revisions: **2 weeks**
Keep Monthly Revisions: **6 months**
Keep Yearly Revisions: **1 year**

A revision is created when the data being backed up is changed. For example, if you backup a file every day and no changes are made for a week, and then you make a change to that file the next week, there is only one revision for that file. The revision is kept through five more changes to the data, and when a sixth change is made, the oldest revision "graduates" to a weekly revision, and that new sixth change becomes a daily revision. This means there are five daily revisions and one weekly revision, or six total revisions. The seventh change to that file will then force the oldest revision to graduate and then there will be five daily and two weekly revisions. When the eighth revision is made, the oldest revision graduates to the monthly revision, so there are five daily, two weekly, and one monthly revision:


Original File
Daily Revisions
Weekly Revisions
Monthly Revisions
Rev1
Rev2
Rev3
Rev4
Rev5
Daily Revisions
Weekly Revisions
Monthly Revisions
Rev2
Rev3
Rev4
Rev5
Rev6
Rev1
Daily Revisions
Weekly Revisions
Monthly Revisions
Rev3
Rev4
Rev5
Rev6
Rev7
Rev2
Rev1
Daily Revisions
Weekly Revisions
Monthly Revisions
Rev4
Rev5
Rev6
Rev7
Rev8
Rev3
Rev2
Rev1

Changing Retention Policies

If you make changes to your retention policy, the updates take effect within 24 hours, at which time, any excess data based on your new policy settings is removed from your device. Note that the removal process can take some time depending on the amount of data. View progress in the **STATUS** page.

Watched Files Page

> This article applies to Barracuda Backup firmware 5.1 and earlier *only*.
>
> The seldomly used Watched Files feature has been deprecated in firmware versions 5.2, and will not be supported for new Barracuda Backup Servers. Note that existing Watched File Rules will continue to function as expected.

Use this page to add files to watch on a particular Barracuda Backup Server. File watch rules are used to monitor and send email alerts when specified files have not been changed often enough or appear smaller than expected. For example, an administrator could choose to receive an alert if third-party backup software fails to process dump files or if the dump files appear to be of insufficient size. Use the **BACKUP > Watched Files** page to add files to watch on a particular Barracuda Backup Server.

Click **Add a File Watch**, and enter the details described in the following table:

Field	Description
Add File Watch Rule Name	Enter a short description for the file watch rule.
Modified Time Threshold	This section displays all data sources set up on the selected Barracuda Backup Server. Select the items to which the watch rule is to apply.
Modified Time Threshold Warning	Turn on **Warn if file is not modified at least once in**, and specify how frequently the file should change in hours, days, weeks, months, or years.
Size Threshold Warning	Turn on **Warn if the size is not at least** and enter the smallest acceptable size for the file in bytes, kilobytes, megabytes, gigabytes, or terabytes.

Click **Save** to save the watch rule, or click **Cancel** to close the page without saving changes.

> ⓘ Note that you can add file watch rules on network file share data sources only; you cannot add a file watch rule on agent data sources.

The **ADMIN > Email Notifications** page allows you to specify the email addresses that are to receive an email notification when files matching the parameters in a file watch rule are detected. The emails are sent to those users who are configured to receive alerts.

RESTORE Page

From the **RESTORE** page you can restore data from the local Barracuda Backup Server, from a remote Barracuda Backup Server that has been used to replicate that system, or from the Barracuda Cloud Storage. Restores from the local Barracuda Backup Server offer the fastest restore times. Multiple methods are available to restore your backed up data. You can restore single files, individual email messages, and entire systems. In firmware version 5.2 and higher, use the **LiveBoot Management** page to manage active virtual machines LiveBooted to the cloud.

In this Section

- VMware Server Recovery and Restoration
- Microsoft Exchange Server Recovery and Restoration
- Microsoft SQL Server Database Recovery and Restoration
- Microsoft Hyper-V Recovery and Restoration
- Microsoft Windows Server Active Directory

- Barracuda LiveBoot in the Cloud
- Barracuda copy.com
- Restore Browser
- How to Restore from Local and Offsite Backups
- How to Recover Backed Up Data
- How to Restore from a Replication Destination
- How to Restore SharePoint Objects Using Kroll Ontrack
- How to Restore a Microsoft Windows Server 2003 Domain Controller
- How to Restore Windows System State
- How to Restore Exchange and GroupWise Messages
- How to Restore a Windows System to Bare Metal
- How to Restore a Linux Server Using Bare Metal Restore
- How to Restore Data with FTPES
- Legacy Firmware Recovery and Restoration Options

> **Legacy Firmware**
> The articles in the Legacy Firmware Recovery and Restoration section refer to firmware version 5.0 or earlier *only*.

Related Articles

- How to Back Up and Restore a Microsoft SharePoint SQL Database
- How to Restore a Microsoft SharePoint SQL Database Using STSADM
- VMware Data Recovery Backup and Restore Permissions

VMware Server Recovery and Restoration

In this Section

- How to Restore a Virtual Machine to its Original Location
- How to Restore a Virtual Machine to a Different Host Protected by Barracuda Backup
- How to Restore a Virtual Machine to an Alternate VMware Host not available through the Barracuda Backup Service
- VMware Data Recovery Licenses
- How to Restore VMware Guest Systems Using Barracuda LiveBoot

How to Restore a Virtual Machine to its Original Location

> This article applies to the Barracuda Backup Server firmware version 4.2, and VMware® 4.0 and above, and the vSphere® Data Recovery API.

Related Articles

- Restore to a Different Host Protected by Barracuda Backup
- Restore to an Alternate VMware Host not available through Barracuda Backup
- Set Up a VMware Server and Guests
- Changed Block Tracking

Barracuda Backup utilizes the vSphere Data Recovery API to backup and restore the VMware Host configuration as well as VMware guests. VMware host backup provides a comprehensive disaster recovery option for virtual machines and provides the ability to recover virtual machines to any VMware host accessible by the Barracuda Backup Server.

Use the Barracuda Backup Server web interface to restore VMware hosts, host configuration, or virtual machine images.

Use the following steps to restore a VMware data source:

1. Log into the Barracuda Backup web interface, and go to the **RESTORE > Restore Browser** page.
2. Expand the VMware data source on the left, and click on the virtual machine you want to restore; all available revisions display.

3. Click **Restore** to the right of the revision to restore.
4. In the **Restore** dialog box, select the following options:
    - **Restore to** - Select **Original Location**
    - **Overwrite** - Turn **On** to overwrite existing data for this virtual machine at the source
5. Click **Start Restoring**.

How to Restore a Virtual Machine to a Different Host Protected by Barracuda Backup

This article applies to the Barracuda Backup Server firmware version 4.2, and VMware® 4.0 and above, and the vSphere® Data Recovery API.

Related Articles

- Restore to Original Location
- Restore to an Alternate VMware Host not available through Barracuda Backup
- Set Up a VMware Server and Guests
- Changed Block Tracking

Barracuda Backup utilizes the vSphere Data Recovery API to protect the VMware guests at the host level. Barracuda Backup provides a comprehensive disaster recovery option for virtual machines and provides the ability to recover virtual machines to any VMware host accessible by the Barracuda Backup Server. Note that the VMware host being restored *must* have a VMware Disaster Recovery and Backup license available from VMware.

Use the following steps to restore a virtual machine to a new location:

1. Log into the Barracuda Backup web interface, and go to the **RESTORE > Restore Browser** page.
2. Expand the VMware data source on the left, and click on the virtual machine you wish to restore; all available revisions display.
3. Click **Restore** to the right of the revision you wish to restore.
4. In the **Restore** dialog box, in the **Restore to** section, select the *second* radio button, and select the host from the drop-down menu.
5. If you are restoring to a vCenter, complete the following steps:
    - From the **Datacenter** drop-down menu, select the data center where you want to restore the virtual machine.
    - From the **Host** drop-down menu, select the desired restore host name.
    - From the **Datastore** drop-down menu, select the desired restore datastore.
6. To overwrite any existing data on the selected virtual machine at the source, turn on **Overwrite**.
7. Click **Start Restoring**.

How to Restore a Virtual Machine to an Alternate VMware Host not available through the Barracuda Backup Service

This article applies to the Barracuda Backup Server firmware version 4.2, and VMware® 4.0 and above, and the vSphere® Data Recovery API.

Related Articles

- Restore to Original Location
- Restore to a Different Host Protected by Barracuda Backup
- Set Up a VMware Server and Guests
- Changed Block Tracking

Barracuda Backup utilizes the vSphere Data Recovery API to backup and restore the VMware Host configuration as well as VMware guests. VMware host backup provides a comprehensive disaster recovery option for virtual machines and provides the ability to recover virtual machines to any VMware host accessible by the Barracuda Backup Server. Note that the VMware host being restored *must* have a VMware Disaster Recovery and Backup license available from VMware.

Use the following steps to restore a virtual machine to an alternate location:

1. Log into the Barracuda Backup web interface, and go to the **RESTORE > Restore Browser** page.
2. Expand the VMware data source on the left, and click on the virtual machine you want to restore; all available revisions display.
3. Click **Restore** to the right of the revision you want to restore.
4. In the **Restore** dialog box, in the **Restore to** section, select the *third* radio button, and enter the fully qualified domain name (FQDN) or IP address of the VMware host where you want to restore the virtual machine.
5. Enter the VMware host username and password in the **Authentication** fields, and click **Load Datacenters** to view a list of datacenters and datastores.
6. If you are restoring to a vCenter, complete the following:
    - From the **Datacenter** drop-down menu, select the data center where you want to restore the virtual machine.
    - From the **Host** drop-down menu, select the desired restore host name.
    - From the **Datastore** drop-down menu, select the desired restore datastore.
7. To overwrite any existing data on the selected virtual machine at the source, turn on **Overwrite**, and click **Start Restoring**.

VMware Data Recovery Licenses

This article refers to Barracuda Backup firmware version 4.2 and higher, and VMware® vSphere®.

Barracuda Backup requires access to the vStorage APIs for Data Protection in order to back up VMware virtual machines. You can access these APIs from the following vSphere Essentials and Acceleration Kits:

- Essentials Kit
- Essentials Plus Kit
- Standard Acceleration Kit
- Enterprise Acceleration Kit
- Enterprise Plus Acceleration Kit

Related Articles

- VMware Data Recovery Backup and Restore Permissions

Additional Resource

- VMware vSphere with Operations Management

How to Restore VMware Guest Systems Using Barracuda LiveBoot

This article refers to firmware 5.0 and higher, and VMware® ESX/ESXi with the VMware license which includes access to vSphere® Data Recovery API.

In this article:

- Restore a Virtual Machine Using Barracuda LiveBoot
- Move the Virtual Machine to a Datastore
- Remove the Virtual Machine from vCenter

Related Articles

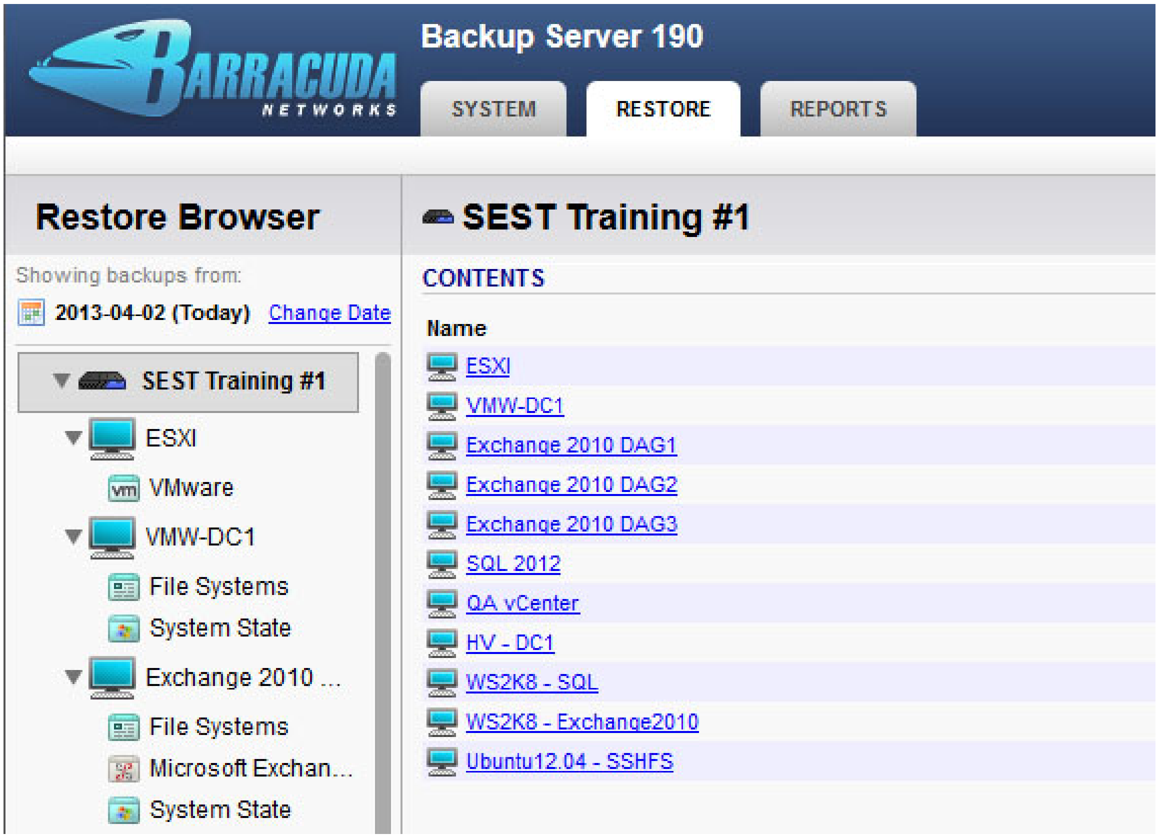
- Understanding Cloud LiveBoot
- How to Use Barracuda LiveBoot in the Cloud
- How to vMotion a LiveBooted Virtual Machine from the Barracuda Backup Server

Use Barracuda LiveBoot to recover and traverse the file structure of VMware virtual guest system data, and to download files and directories within a VMware snapshot. In the event of a failure with your primary storage system, the Barracuda Backup Server can act as the datastore for your VMware ESX/ESXi server. You can recover any revision of a VMware virtual guest server within your retention policy, and serve up deduplicated content as needed by the virtual server.

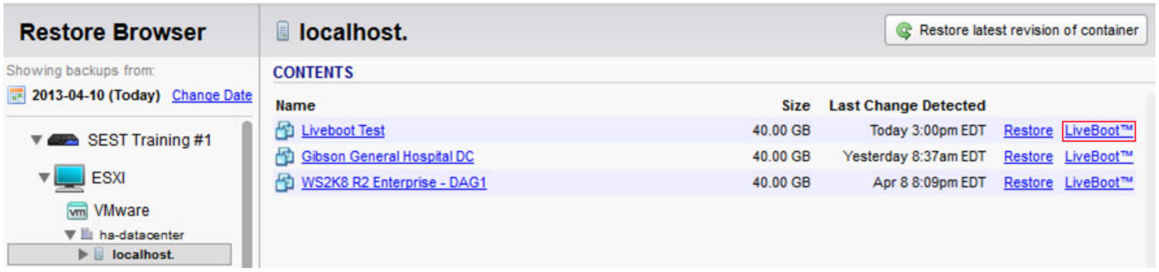
Restore a Virtual Machine Using Barracuda LiveBoot

Use the following steps to recover VMware virtual guest system data using Barracuda LiveBoot:

1. Log in to the Barracuda Backup web interface, and go to **RESTORE**:

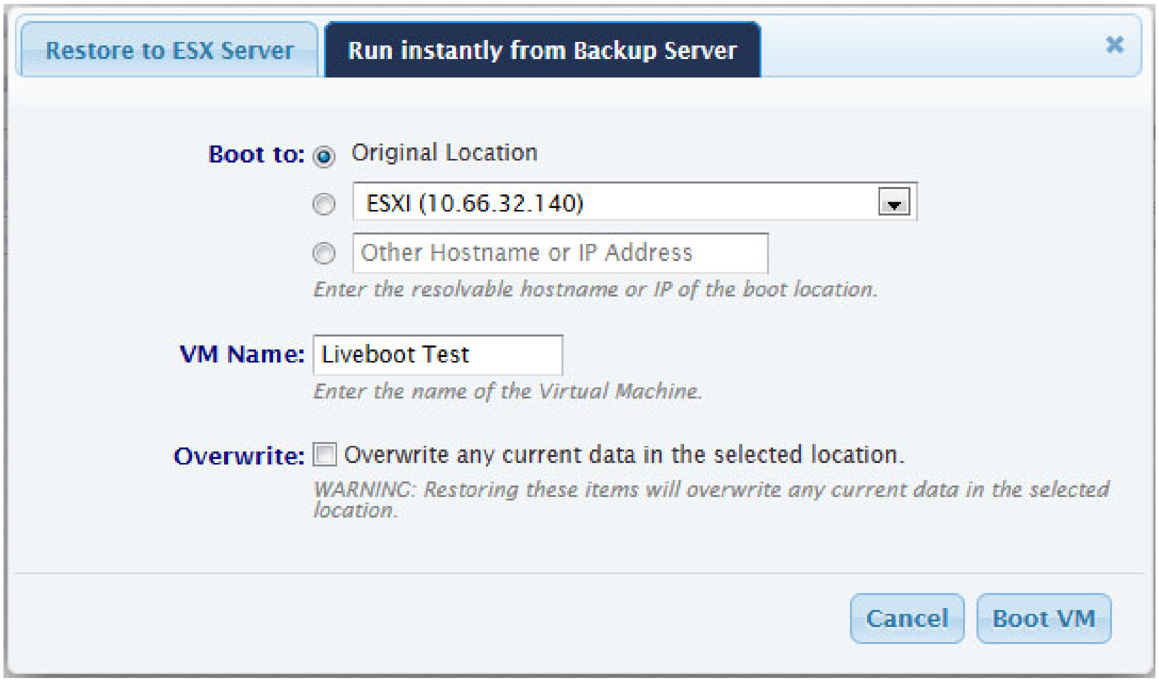

BARRACUDA NETWORKS
Backup Server 190
SYSTEM
RESTORE
REPORTS
Restore Browser
Showing backups from:
2013-04-02 (Today) Change Date
SEST Training #1
ESXI
VMware
VMW-DC1
File Systems
System State
Exchange 2010 ...
File Systems
Microsoft Exchan...
System State
SEST Training #1
CONTENTS
Name
ESXI
VMW-DC1
Exchange 2010 DAG1
Exchange 2010 DAG2
Exchange 2010 DAG3
SQL 2012
QA vCenter
HV - DC1
WS2K8 - SQL
WS2K8 - Exchange2010
Ubuntu12.04 - SSHFS

2. Navigate to and expand the ESXi host, click on the guest system to restore, and drill down to the level you want to restore.
3. Click the **LiveBoot** link next to the Virtual Machine to restore:


Restore Browser
Showing backups from:
2013-04-10 (Today) Change Date
SEST Training #1
ESXI
VMware
ha-datacenter
localhost.
localhost.
Restore latest revision of container
CONTENTS

Name	Size	Last Change Detected		
Liveboot Test	40.00 GB	Today 3:00pm EDT	Restore	LiveBoot™
Gibson General Hospital DC	40.00 GB	Yesterday 8:37am EDT	Restore	LiveBoot™
WS2K8 R2 Enterprise - DAG1	40.00 GB	Apr 8 8:09pm EDT	Restore	LiveBoot™

4. The **Run Instantly from Backup Server** page displays:

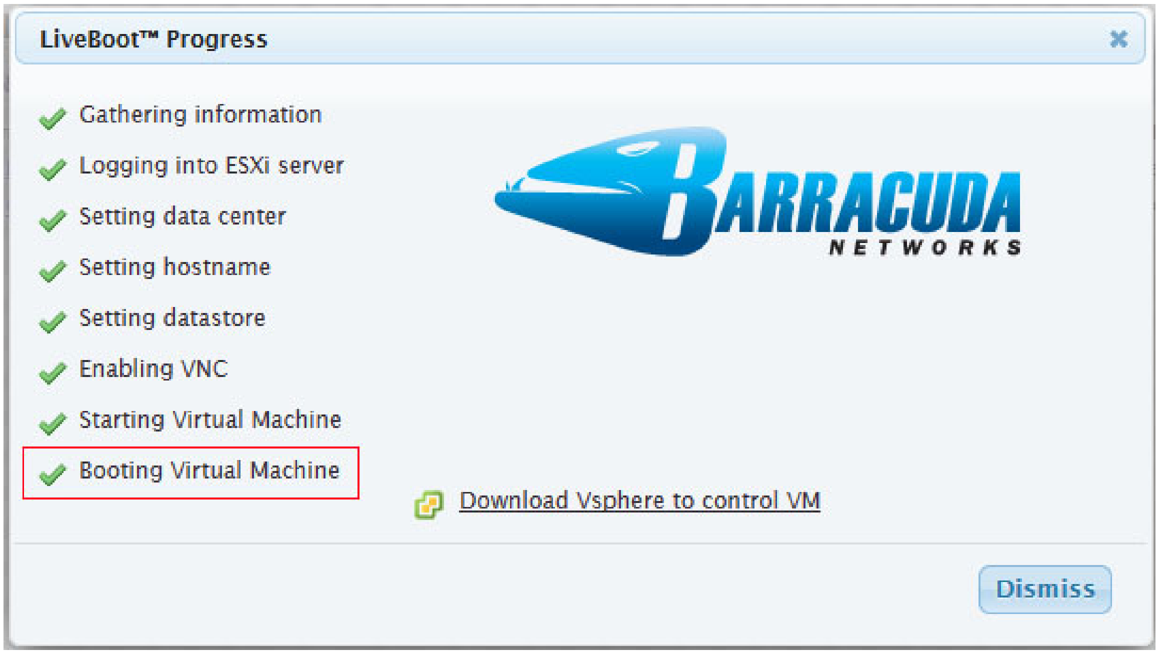


Boot to: ● Original Location
○ ESXI (10.66.32.140)
○ Other Hostname or IP Address
Enter the resolvable hostname or IP of the boot location.

VM Name: Liveboot Test
Enter the name of the Virtual Machine.

Overwrite: ☐ Overwrite any current data in the selected location.
WARNING: Restoring these items will overwrite any current data in the selected location.

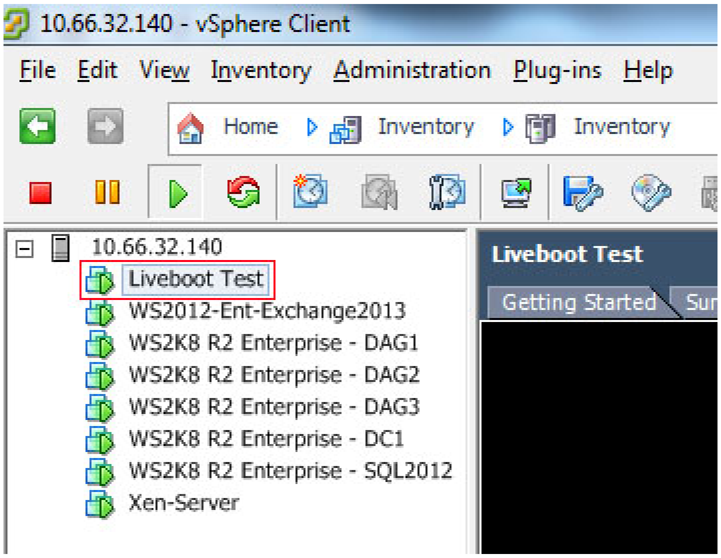
5. In the **Boot to** section, select whether to boot the Virtual Machine to the **Original Location** or enter an alternate Hostname or IP address.
6. Enter name of the Virtual Machine in the **VM Name** field, for example, `LiveBootRestore`, and click **Boot VM**.
7. The progress dialog box displays. Once the process is complete, a green check mark displays next to **Booting Virtual Machine**:



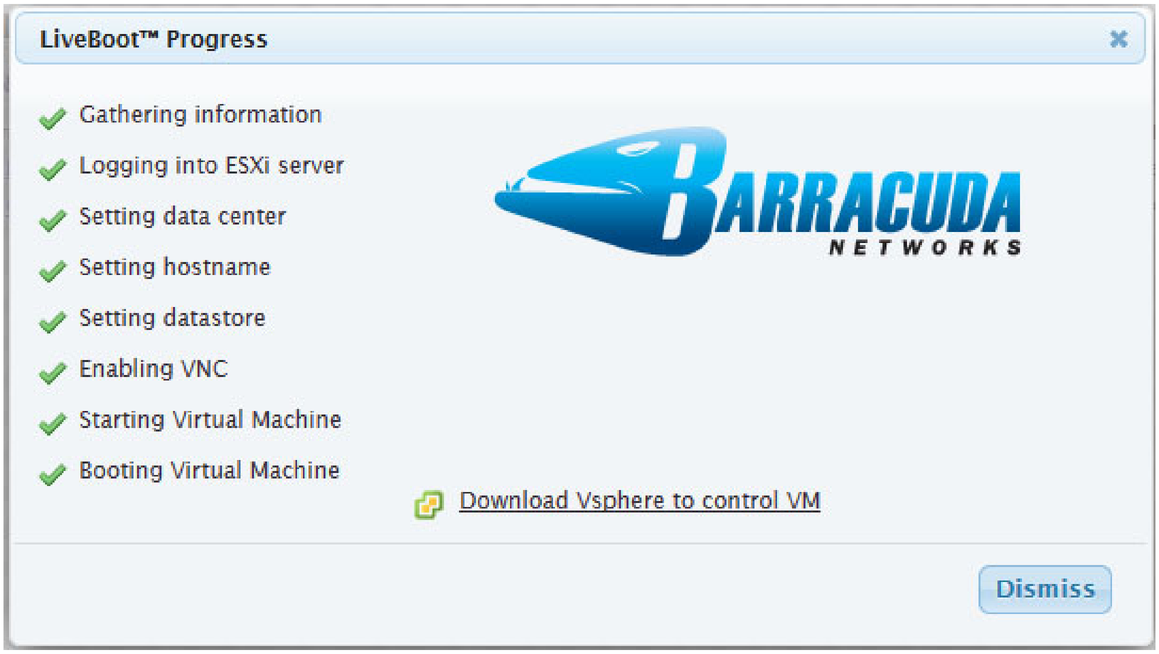
LiveBoot™ Progress

✓ Gathering information
✓ Logging into ESXi server
✓ Setting data center
✓ Setting hostname
✓ Setting datastore
✓ Enabling VNC
✓ Starting Virtual Machine
✓ Booting Virtual Machine

8. Once the process is complete the server boots up.
9. On your VMware Server, open VCenter vSphere Client and verify the Virtual Machine displays:


10.66.32.140 - vSphere Client
File
Edit
View
Inventory
Administration
Plug-ins
Help
Home
Inventory
Inventory
10.66.32.140
Liveboot Test
WS2012-Ent-Exchange2013
WS2K8 R2 Enterprise - DAG1
WS2K8 R2 Enterprise - DAG2
WS2K8 R2 Enterprise - DAG3
WS2K8 R2 Enterprise - DC1
WS2K8 R2 Enterprise - SQL2012
Xen-Server
Liveboot Test
Getting Started
Sur

10. In the Barracuda Backup web interface, click **Dismiss** in the **LiveBoot Progress** dialog box:

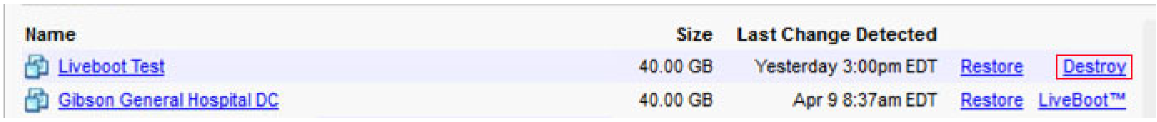


LiveBoot™ Progress

- ✓ Gathering information
- ✓ Logging into ESXi server
- ✓ Setting data center
- ✓ Setting hostname
- ✓ Setting datastore
- ✓ Enabling VNC
- ✓ Starting Virtual Machine
- ✓ Booting Virtual Machine

BARRACUDA
NETWORKS
Download Vsphere to control VM
Dismiss

11. Once the LiveBoot is complete, in the Barracuda Backup web interface click **Destroy** to terminate the process:

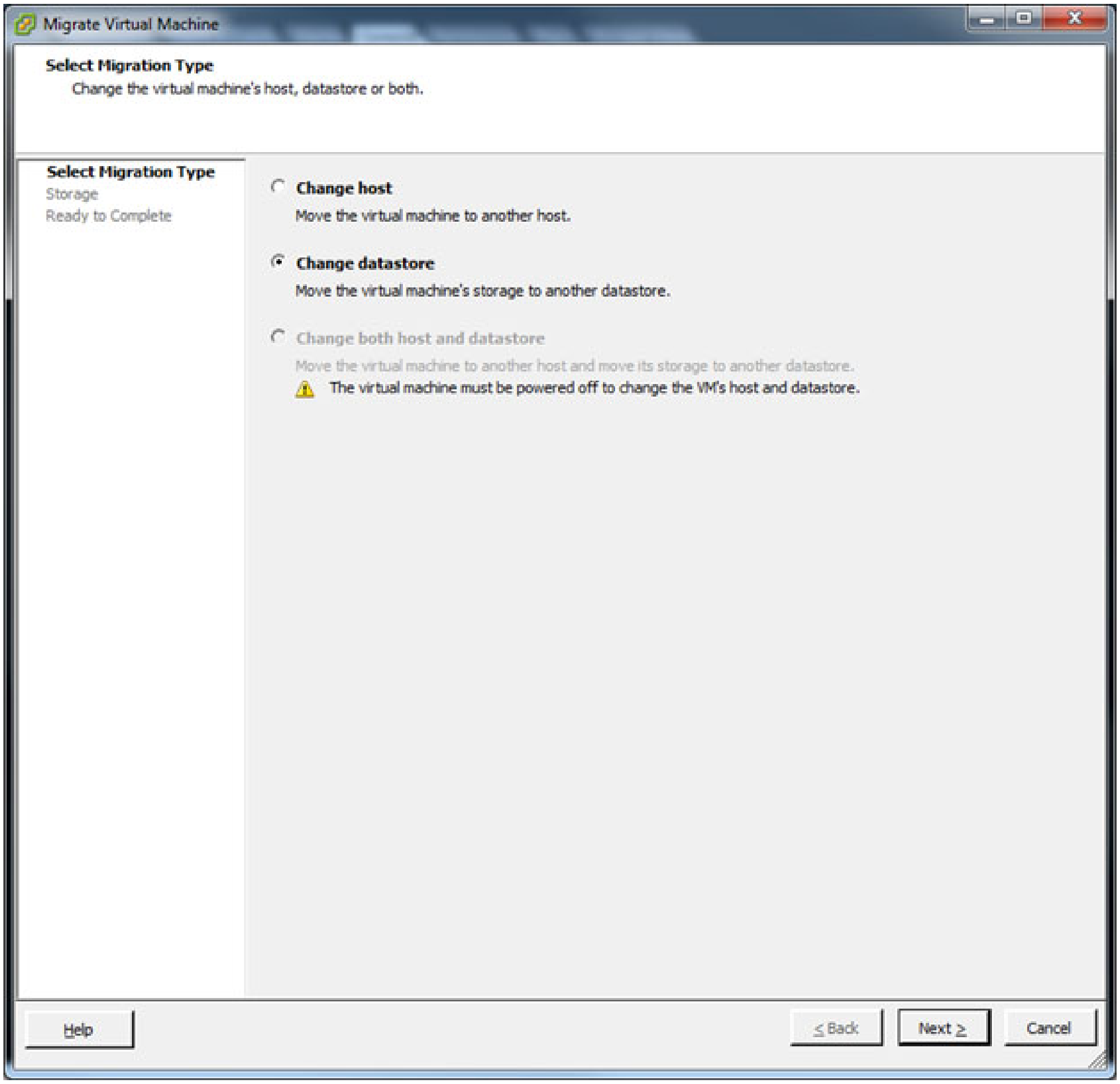


Name	Size	Last Change Detected		
Liveboot Test	40.00 GB	Yesterday 3:00pm EDT	Restore	Destroy
Gibson General Hospital DC	40.00 GB	Apr 9 8:37am EDT	Restore	LiveBoot™

Move the Virtual Machine to a Datastore

Use the following steps to move the "LiveBooted" Virtual Machine to your own datastore.

1. On your VMware Server, open the VCenter VSphere Client.
2. Right-click on the Virtual Machine and click **Migrate**. The **Migrate Virtual Machine** wizard displays.
3. In the **Select Migration type** page, select **Change datastore**:


Migrate Virtual Machine

Select Migration Type

Change the virtual machine's host, datastore or both.

Select Migration Type
Storage
Ready to Complete

○ **Change host**

Move the virtual machine to another host.

● **Change datastore**

Move the virtual machine's storage to another datastore.

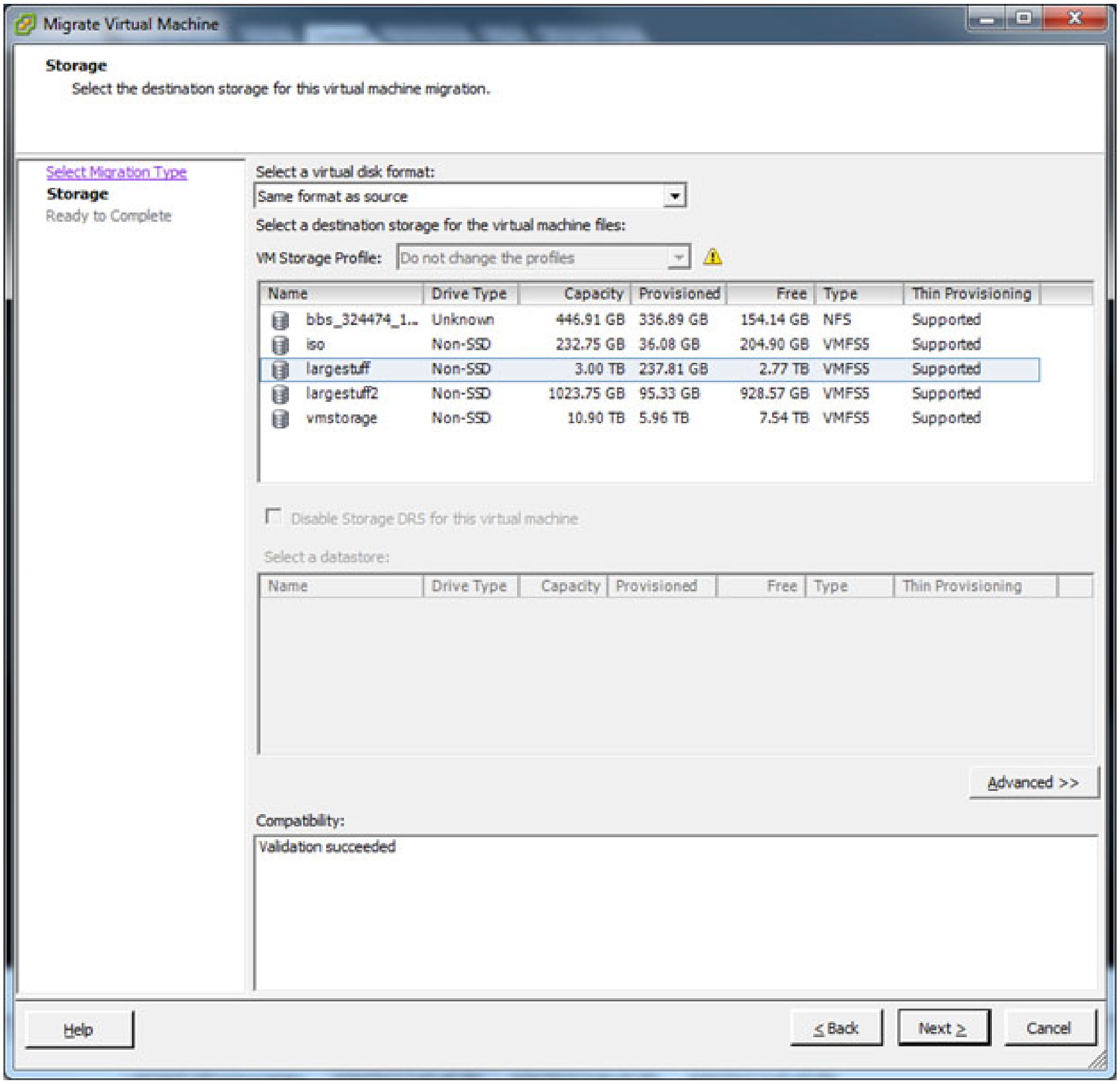
○ **Change both host and datastore**

Move the virtual machine to another host and move its storage to another datastore.

⚠ The virtual machine must be powered off to change the VM's host and datastore.

Help
≤ Back
Next ≥
Cancel

4. Click **Next**. In the **Storage** page, select the datastore to which to move the Virtual Machine:



Storage

Select the destination storage for this virtual machine migration.

Select a virtual disk format: Same format as source

Select a destination storage for the virtual machine files:

VM Storage Profile: Do not change the profiles

Name	Drive Type	Capacity	Provisioned	Free	Type	Thin Provisioning
bbs_324474_1...	Unknown	446.91 GB	336.89 GB	154.14 GB	NFS	Supported
iso	Non-SSD	232.75 GB	36.08 GB	204.90 GB	VMFS5	Supported
largestuff	Non-SSD	3.00 TB	237.81 GB	2.77 TB	VMFS5	Supported
largestuff2	Non-SSD	1023.75 GB	95.33 GB	928.57 GB	VMFS5	Supported
vmstorage	Non-SSD	10.90 TB	5.96 TB	7.54 TB	VMFS5	Supported

☐ Disable Storage DRS for this virtual machine

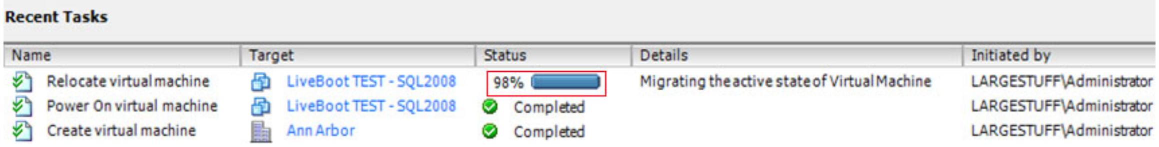
Select a datastore:

Name	Drive Type	Capacity	Provisioned	Free	Type	Thin Provisioning

Compatibility:

Validation succeeded

5. Click **Next**. In the **Ready to Complete** page, click **Finish** to start the migration process using vMotion.
6. You can check the progress of vMotion in the **Recent Tasks** log:



Recent Tasks

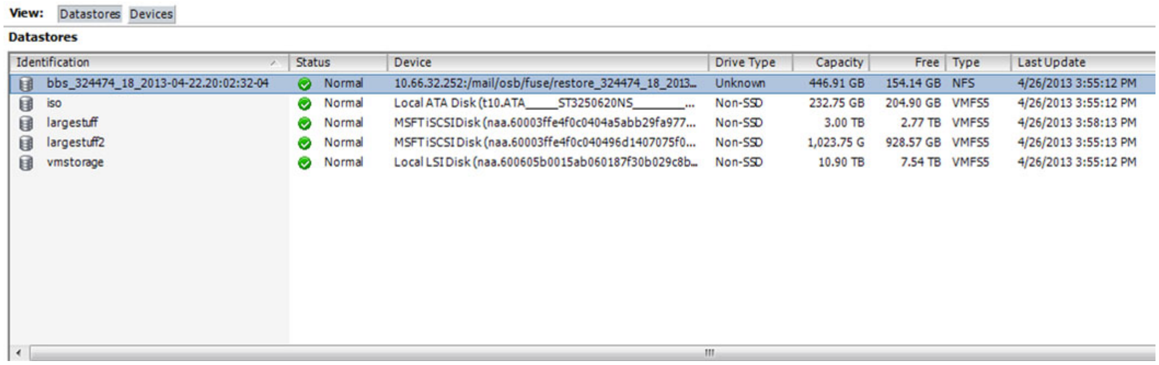
Name	Target	Status	Details	Initiated by
Relocate virtual machine	LiveBoot TEST - SQL2008	98%	Migrating the active state of Virtual Machine	LARGESTUFF\Administrator
Power On virtual machine	LiveBoot TEST - SQL2008	Completed		LARGESTUFF\Administrator
Create virtual machine	Ann Arbor	Completed		LARGESTUFF\Administrator

7. Select the active environment to which to move the restored system, click **Next**, and then click **Finish**.

Remove the Virtual Machine from vCenter

Use the following steps to remove the "LiveBooted" Virtual Machine from vCenter:

1. On your VMware Server, open the VCenter VSphere Client.
2. Right-click on the LiveBooted Virtual Machine and click **Power off**.
3. Right-click the Virtual Machine again and click **Delete from disk**.
4. Click on the ESXi host where the Virtual Machine was running, and click the **Configuration** tab:


View: Datastores Devices
Datastores

Identification	Status	Device	Drive Type	Capacity	Free	Type	Last Update
bbs_324474_18_2013-04-22.20:02:32-04	Normal	10.66.32.252:/mail/osb/fuse/restore_324474_18_2013...	Unknown	446.91 GB	154.14 GB	NFS	4/26/2013 3:55:12 PM
iso	Normal	Local ATA Disk (t10.ATA_____ST3250620NS________...	Non-SSD	232.75 GB	204.90 GB	VMFS5	4/26/2013 3:55:12 PM
largestuff	Normal	MSFT iSCSIDisk (naa.60003ffe4f0c0404a5abb29fa977...	Non-SSD	3.00 TB	2.77 TB	VMFS5	4/26/2013 3:58:13 PM
largestuff2	Normal	MSFT iSCSI Disk (naa.60003ffe4f0c040496d1407075f0...	Non-SSD	1,023.75 G	928.57 GB	VMFS5	4/26/2013 3:55:13 PM
vmstorage	Normal	Local LSI Disk (naa.600605b0015ab060187f30b029c8b...	Non-SSD	10.90 TB	7.54 TB	VMFS5	4/26/2013 3:55:12 PM

5. Right-click on the LiveBooted Virtual Machine datastore, and click **Unmount**.

Microsoft Exchange Server Recovery and Restoration

In this Section

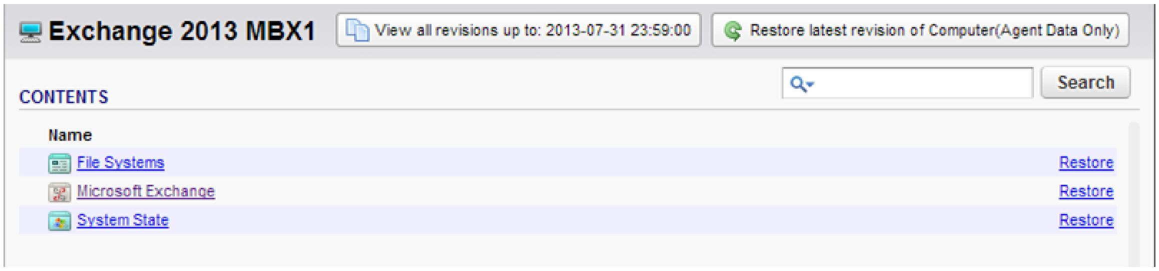
- How to Restore a Microsoft Exchange 2013 Server Database to a Recovery Storage Group
- How to Restore a Microsoft Exchange 2010 Server by Overwriting an Existing Database
- How to Restore a Microsoft Exchange 2010 Server to a Recovery Database
- How to Restore a Microsoft Exchange 2007 Database
- How to Restore a Microsoft Exchange 2003 Database by Overwriting Existing Database
- How to Restore a Microsoft Exchange 2003 Database using a Recovery Storage Group

How to Restore a Microsoft Exchange 2013 Server Database to a Recovery Storage Group

> This article refers to Barracuda Backup version 5.3 or higher, and Microsoft® Exchange Server 2013. This article assumes the Microsoft Exchange Server is installed and configured.

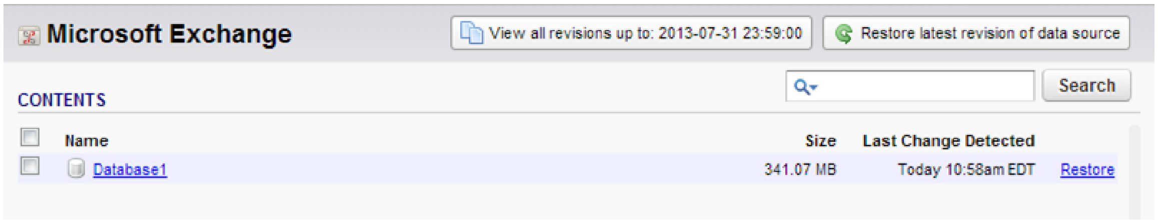
Set up Barracuda Backup

1. Log in to **Barracuda Backup**, and select the Barracuda Backup Server that contains the Microsoft Exchange 2013 Server backups that you wish to restore.
2. Go to the **RESTORE** **> Restore Browser** page, select the **Microsoft Exchange** data source, and click **Microsoft Exchange**:


Exchange 2013 MBX1
View all revisions up to: 2013-07-31 23:59:00
Restore latest revision of Computer(Agent Data Only)
CONTENTS
Search

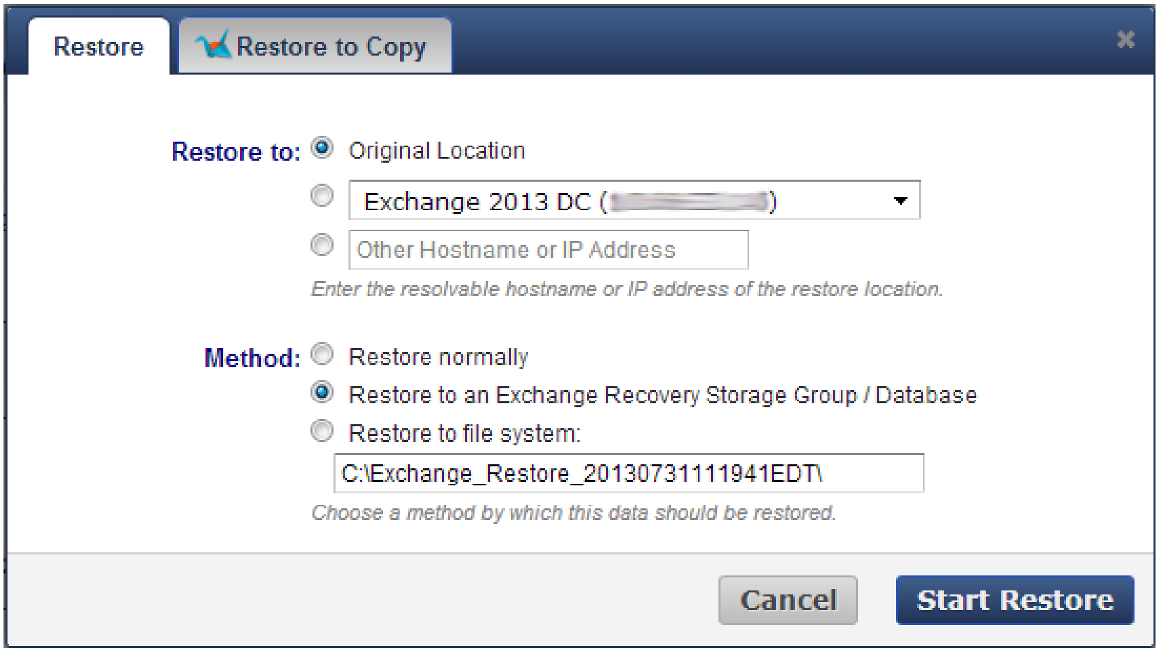
Name	
File Systems	Restore
Microsoft Exchange	Restore
System State	Restore

3. To restore the latest backed up database, click **Restore**:


Microsoft Exchange
View all revisions up to: 2013-07-31 23:59:00
Restore latest revision of data source
CONTENTS
Search

☐	Name	Size	Last Change Detected	
☐	Database1	341.07 MB	Today 10:58am EDT	Restore

4. The Restore window displays. In the **Restore to** section, select **Restore to an Exchange Recovery Storage Group / Database**:



Restore to: ● Original Location
○ Exchange 2013 DC ([redacted])
○ Other Hostname or IP Address
Enter the resolvable hostname or IP address of the restore location.

Method: ○ Restore normally
● Restore to an Exchange Recovery Storage Group / Database
○ Restore to file system:
C:\Exchange_Restore_20130731111941EDT\
Choose a method by which this data should be restored.

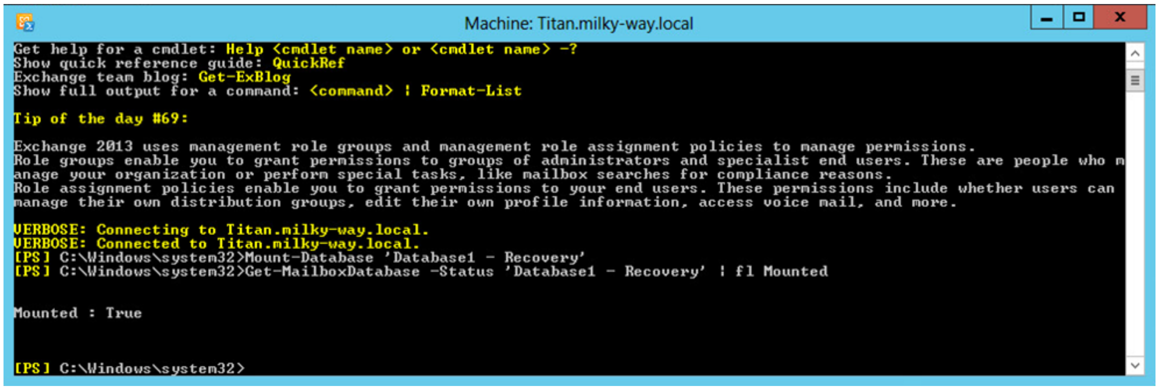
5. Click **Start Restore**. Once the restore is complete, go to **REPORTS > Restore** to verify the restore completed successfully.

Recover a Mailbox from the Exchange 2013 Recovery Storage Group

ⓘ When running the commands in this section, substitute *DatabaseName* with the name of your original database.

1. Log in to the Exchange 2013 Mailbox Server, and open the Exchange Management Shell.
2. To mount your recovery database, run the following command:

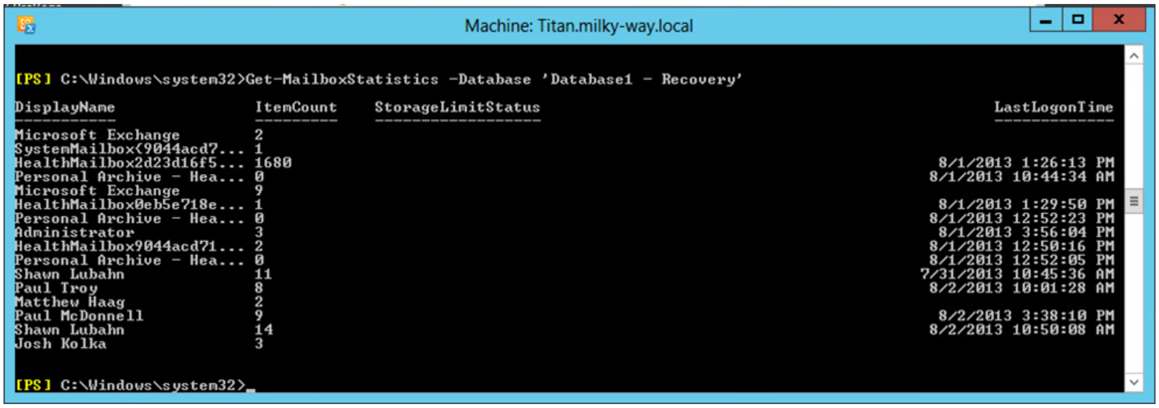
```
Mount-Database 'DatabaseName - Recovery'
```



```
Get help for a cmdlet: Help <cmdlet name> or <cmdlet name> -?
Show quick reference guide: QuickRef
Exchange team blog: Get-ExBlog
Show full output for a command: <command> | Format-List

Tip of the day #69:

Exchange 2013 uses management role groups and management role assignment policies to manage permissions.
Role groups enable you to grant permissions to groups of administrators and specialist end users. These are people who m
anage your organization or perform special tasks, like mailbox searches for compliance reasons.
Role assignment policies enable you to grant permissions to your end users. These permissions include whether users can
manage their own distribution groups, edit their own profile information, access voice mail, and more.

VERBOSE: Connecting to Titan.milky-way.local.
VERBOSE: Connected to Titan.milky-way.local.
[PS] C:\Windows\system32>Mount-Database 'Database1 - Recovery'
[PS] C:\Windows\system32>Get-MailboxDatabase -Status 'Database1 - Recovery' | fl Mounted


Mounted : True


[PS] C:\Windows\system32>
```

3. To view the Mailboxes within the database, run the following command:

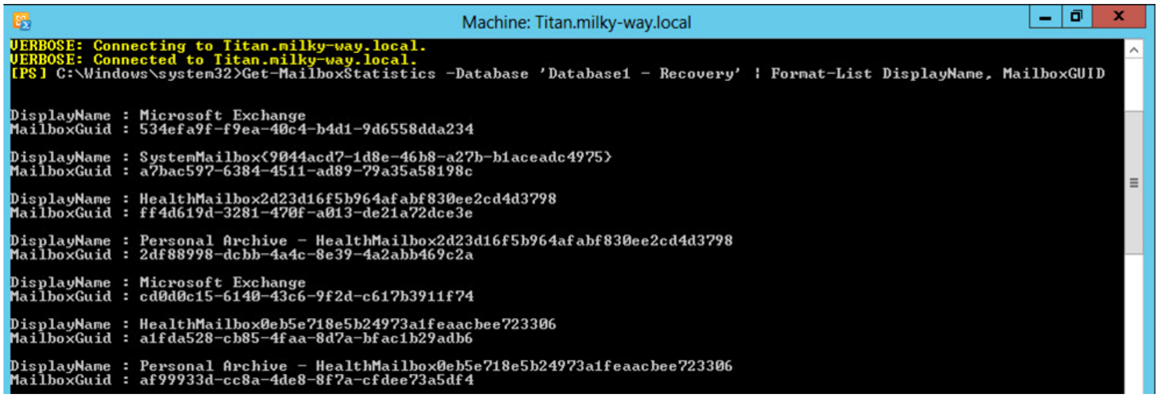
```
Get-MailboxStatistics -Database 'DatabaseName - Recovery'
```



```

[PS] C:\Windows\system32>Get-MailboxStatistics -Database 'Database1 - Recovery'

DisplayName               ItemCount    StorageLimitStatus                                                  LastLogonTime
-----------               ---------    ------------------                                                  -------------
Microsoft Exchange        2
SystemMailbox<9044acd7... 1
HealthMailbox2d23d16f5... 1680                                                                        8/1/2013 1:26:13 PM
Personal Archive - Hea... 0                                                                          8/1/2013 10:44:34 AM
Microsoft Exchange        9
HealthMailbox0eb5e718e... 1                                                                           8/1/2013 1:29:50 PM
Personal Archive - Hea... 0                                                                          8/1/2013 12:52:23 PM
Administrator             3                                                                           8/1/2013 3:56:04 PM
HealthMailbox9044acd71... 2                                                                          8/1/2013 12:50:16 PM
Personal Archive - Hea... 0                                                                          8/1/2013 12:52:05 PM
Shawn Lubahn              11                                                                        7/31/2013 10:45:36 AM
Paul Troy                 8                                                                          8/2/2013 10:01:28 AM
Matthew Haag              2
Paul McDonnell            9                                                                           8/2/2013 3:38:10 PM
Shawn Lubahn              14                                                                         8/2/2013 10:50:08 AM
Josh Kolka                3

[PS] C:\Windows\system32>_
```

4. To view the globally unique identifier (GUID), run the following command:

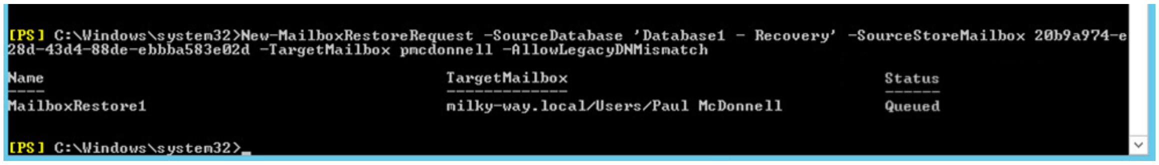
```
Get-MailboxStatistics -Database 'DatabaseName - Recovery' | Format-List
DisplayName, MailboxGUID
```



```
VERBOSE: Connecting to Titan.milky-way.local.
VERBOSE: Connected to Titan.milky-way.local.
[PS] C:\Windows\system32>Get-MailboxStatistics -Database 'Database1 - Recovery' | Format-List DisplayName, MailboxGUID

DisplayName : Microsoft Exchange
MailboxGuid : 534efa9f-f9ea-40c4-b4d1-9d6558dda234

DisplayName : SystemMailbox{9044acd7-1d8e-46b8-a27b-b1aceadc4975}
MailboxGuid : a7bac597-6384-4511-ad89-79a35a58198c

DisplayName : HealthMailbox2d23d16f5b964afabf830ee2cd4d3798
MailboxGuid : ff4d619d-3281-470f-a013-de21a72dce3e

DisplayName : Personal Archive - HealthMailbox2d23d16f5b964afabf830ee2cd4d3798
MailboxGuid : 2df88998-dcbb-4a4c-8e39-4a2abb469c2a

DisplayName : Microsoft Exchange
MailboxGuid : cd0d0c15-6140-43c6-9f2d-c617b3911f74

DisplayName : HealthMailbox0eb5e718e5b24973a1feaacbee723306
MailboxGuid : a1fda528-cb85-4faa-8d7a-bfac1b29adb6

DisplayName : Personal Archive - HealthMailbox0eb5e718e5b24973a1feaacbee723306
MailboxGuid : af99933d-cc8a-4de8-8f7a-cfdee73a5df4
```

5. To restore a mailbox using the GUID, run the following command:

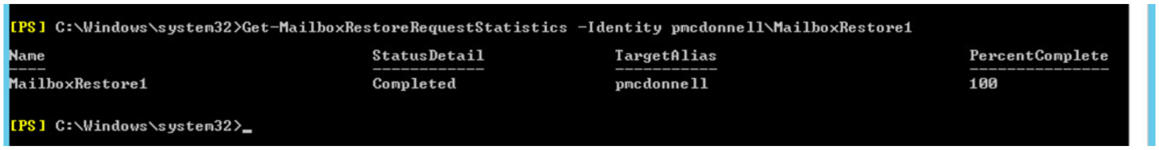
```
New-MailboxRestoreRequest -SourceDatabase 'DatabaseName - Recovery'
-SourceStoreMailbox MailboxGUID -TargetMailbox TargetMailboxAlias -AllowLegacyDN
Mismatch
```



```
[PS] C:\Windows\system32>New-MailboxRestoreRequest -SourceDatabase 'Database1 - Recovery' -SourceStoreMailbox 20b9a974-e
28d-43d4-88de-ebbba583e02d -TargetMailbox pmcdonnell -AllowLegacyDNMismatch

Name                                           TargetMailbox                                  Status
----                                           -------------                                  ------
MailboxRestore1                                milky-way.local/Users/Paul McDonnell           Queued


[PS] C:\Windows\system32>_
```

6. To check the status of your Mailbox restore, run the following command:

```
Get-MailboxRestoreRequestStatistics -Identity MailboxUser\RestoreRequestName
```



```
[PS] C:\Windows\system32>Get-MailboxRestoreRequestStatistics -Identity pmcdonnell\MailboxRestore1

Name                                   StatusDetail              TargetAlias                          PercentComplete
----                                   ------------              -----------                          ---------------
MailboxRestore1                        Completed                 pmcdonnell                           100


[PS] C:\Windows\system32>_
```

How to Restore a Microsoft Exchange 2010 Server by Overwriting an Existing Database

This article refers to Barracuda Backup firmware 4.0 and higher, and Microsoft® Exchange 2010 Server. This article assumes the Microsoft Exchange Server is installed and configured. This article describes how to restore an Exchange 2010 Server by overwriting an existing database or to an original location. You can also restore to a Recovery Storage Group (RSG).

In this article:

- Step 1. Allow Database Restore
- Step 2. Specify Barracuda Backup Restore Settings
- Step 3. Mount the Database

Related Articles
- Restore to a Recovery Database

Additional Resource
- How do I set up my Barracuda Backup Service to restore Exchange 2010?

Warning
This option overwrites *all* existing data. If you do not want to overwrite the database, see Restore to a Recovery Storage Group.

Take caution when overwriting an existing database; Barracuda Networks highly recommends restoring to a separate recovery database except in cases of extreme data loss or when performing disaster recovery.

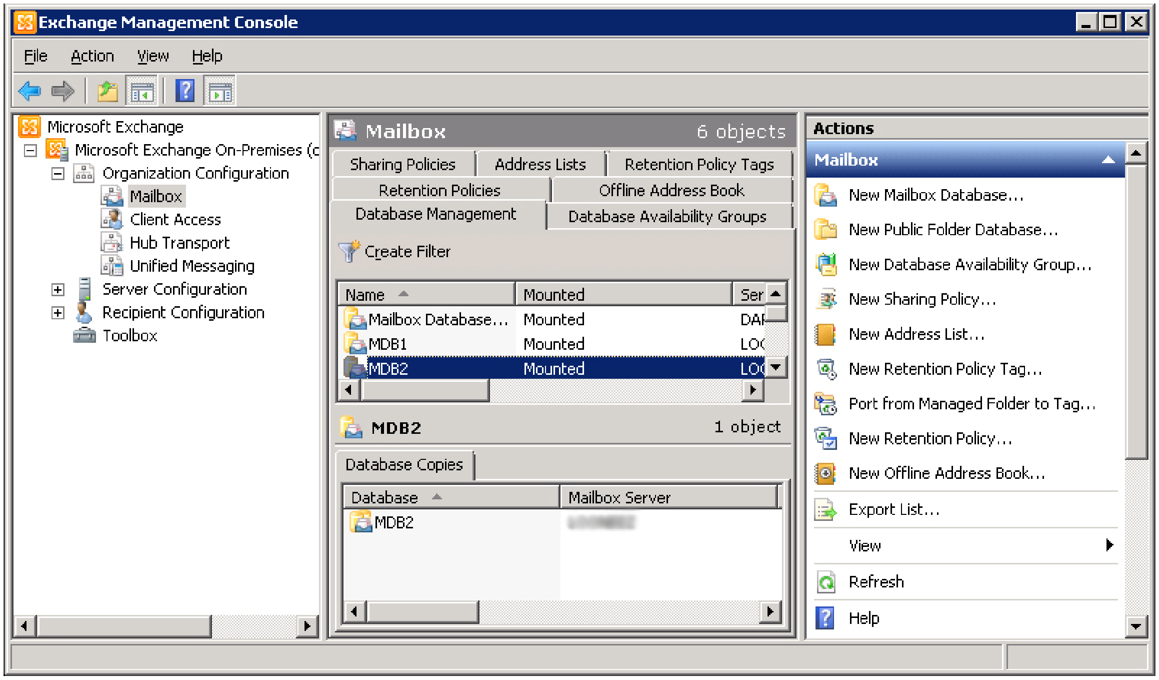
If you do not want to restore your Exchange Server by overwriting the existing database, you can select a different option:

- Restore Exchange 2010 to Recovery Database
- Restore Single Exchange 2010 Mailbox
- Restore All Exchange 2010 Mailboxes

See Restore to a Recovery Storage Group for more information on these options.

Step 1. Allow Database Restore

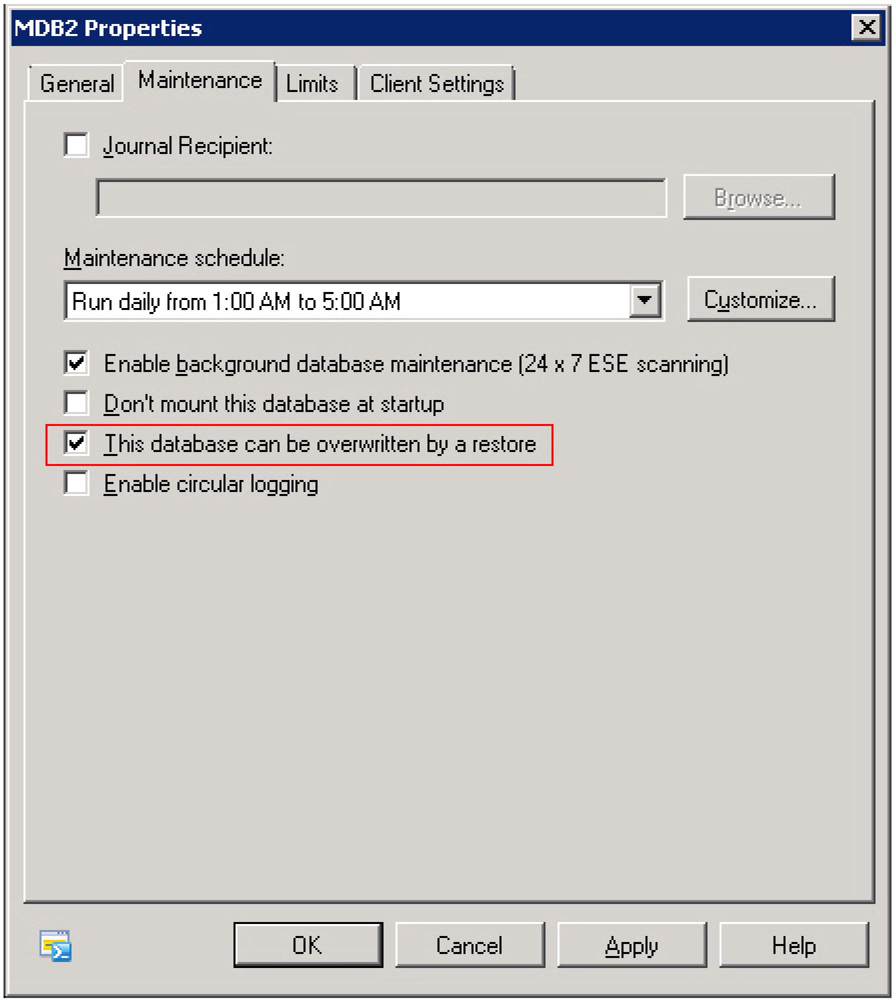
1. Log in to your Exchange Server as the administrator, and open the Exchange Management Console (EMC) from **Start > All Programs > Microsoft Exchange Server > Exchange Management Console**.
2. In the left pane, expand **Microsoft Exchange > Microsoft Exchange On-Premises > Organization Configuration**, and click **Mailbox**:


Exchange Management Console
File
Action
View
Help
Microsoft Exchange
Microsoft Exchange On-Premises (c
Organization Configuration
Mailbox
Client Access
Hub Transport
Unified Messaging
Server Configuration
Recipient Configuration
Toolbox
Mailbox
6 objects
Sharing Policies
Address Lists
Retention Policy Tags
Retention Policies
Offline Address Book
Database Management
Database Availability Groups
Create Filter
MDB2
1 object
Database Copies
Actions
Mailbox
New Mailbox Database...
New Public Folder Database...
New Database Availability Group...
New Sharing Policy...
New Address List...
New Retention Policy Tag...
Port from Managed Folder to Tag...
New Retention Policy...
New Offline Address Book...
Export List...
View
Refresh
Help

Name	Mounted	Ser
Mailbox Database...	Mounted	DAF
MDB1	Mounted	LOC
MDB2	Mounted	LOC

Database	Mailbox Server
MDB2	

3. In the center pane, right-click the mailbox database you want to overwrite with the restore, and click **Properties**.
4. In the **Mailbox Database** dialog box, click the **Maintenance** tab, and select **This database can be overwritten by a restore**:


MDB2 Properties
General
Maintenance
Limits
Client Settings
Browse...
Customize...
OK
Cancel
Apply
Help

☐ Journal Recipient:

Maintenance schedule: Run daily from 1:00 AM to 5:00 AM

☑ Enable background database maintenance (24 x 7 ESE scanning)

☐ Don't mount this database at startup

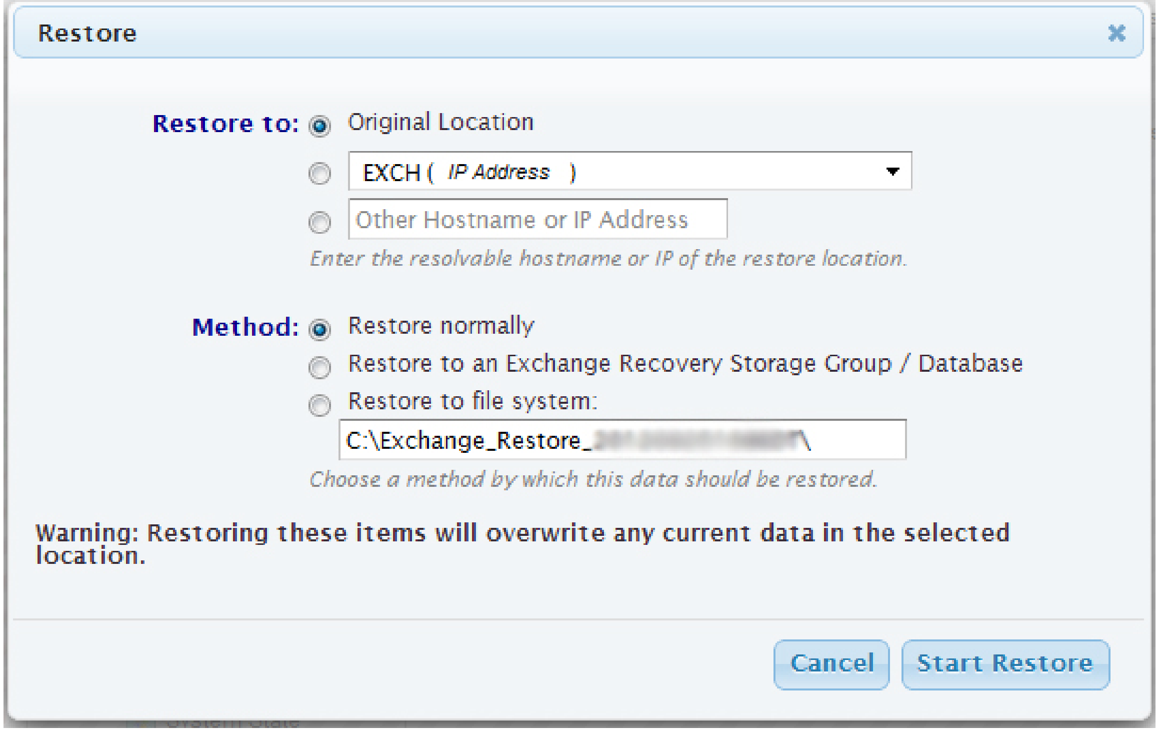
☑ This database can be overwritten by a restore

☐ Enable circular logging

5. Click **Apply**, and then click **OK** to close the dialog box.
6. Right-click the database, and click **Unmount**.

Step 2. Specify Barracuda Backup Restore Settings

1. Log in to Barracuda Backup web interface, and select the associated Barracuda Backup Server in the left pane.
2. Go to **RESTORE > Restore Browser**. Locate the Exchange 2010 Server, and click **Restore**.
3. In the **Restore** dialog box, choose the **Restore to** location:
   - Original Location
   - Select an IP Address from the available servers
   - Enter an IP Address or FDQDN
4. Choose the Restore method as **Restore normally**, and click **Start Restore**.



Restore to: ● Original Location
○ EXCH (*IP Address*)
○ Other Hostname or IP Address
Enter the resolvable hostname or IP of the restore location.

Method: ● Restore normally
○ Restore to an Exchange Recovery Storage Group / Database
○ Restore to file system:
C:\Exchange_Restore_[redacted]\
Choose a method by which this data should be restored.

Warning: Restoring these items will overwrite any current data in the selected location.

5. Go to the **REPORTS > Restore** page to monitor the restore progress.

Step 3. Mount the Database

Once the restore is complete, use the following steps to mount the database.

1. Log in to the target Exchange 2010 Server as the Administrator, and open the EMC.
2. In the left pane, expand **Microsoft Exchange > Microsoft Exchange On-Premises > Organization Configuration**, and click **Mailbox**.
3. In the center pane, click the **Mailbox Database** that was restored, and in the right pane, click **Mount Database**.
4. The database should now be ready to use; ensure users can access their mailboxes.

How to Restore a Microsoft Exchange 2010 Server to a Recovery Database

This article refers to Barracuda Backup firmware 4.0 and higher, and Microsoft ® Exchange® 2010 Server. This article assumes the Microsoft Exchange Server is installed and configured. This article describes how to restore a Microsoft Exchange 2010 Server to a Recovery Storage Group. You can also restore a Microsoft Exchange 2010 Server by overwriting an existing database or restoring to an original location.

In this article:

- Step 1. Barracuda Backup Setup
- Step 2. Microsoft Exchange 2010 Server
- Step 3. Restore Microsoft Exchange 2010 Mailboxes
    - Option 1. Restore a Single Exchange 2010 Mailbox
    - Option 2. Restore All Exchange 2010 Mailboxes

Related Articles
• Restore by Overwriting the Database

Additional Resource
- How do I set up my Barracuda Backup Service to restore Exchange 2010?

Recovery Storage Group
If you do not create a recovery storage group, Barracuda Backup creates one and places it in the default Exchange install location. If you want to create a recovery storage database, use the following Exchange PowerShell command, replacing the bracketed variables with the actual database and server names:

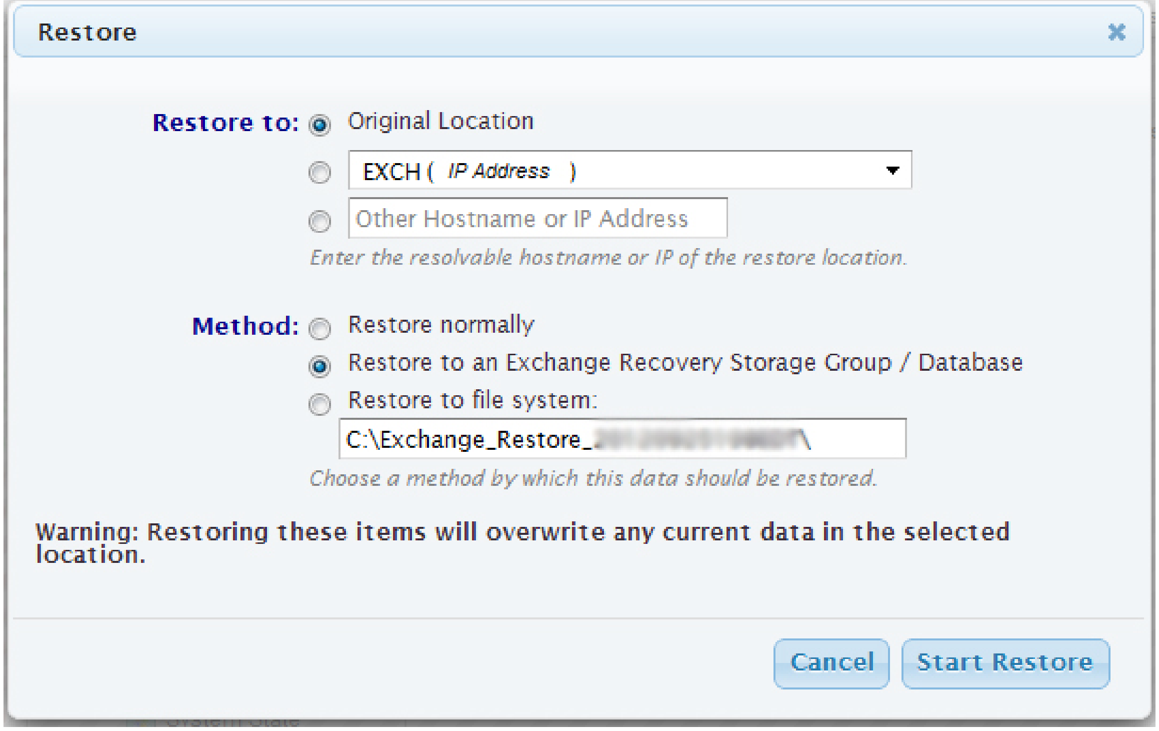
```
New-MailboxDatabase -Recovery -Name "<atabasename - Recovery" -Server servername -EdbFilePath "R:\databasename - Recovery\databasename - Recovery.edb" -LogFolderPath "R:\databasename - Recovery"
```

Step 1. Barracuda Backup Setup

1. Log in to **Barracuda Backup**, and select the Barracuda Backup Server that contains the Microsoft Exchange 2010 Server backups you want to restore.
2. Go to the **Restore > Restore Browser** page, and select the **Microsoft Exchange** data source; the backed up Exchange 2010 databases display.
3. To restore the latest backed up database, click **Restore**. The Restore window displays. In the **Restore to** section, select **Original Location**.

> If restoring to a server with a different IP address, select the drop down menu, and select the associated Exchange Server from the list.

4. Next to the Method section, select **Restore to an Exchange Recovery Storage Group / Database**:



Restore

Restore to: ● Original Location
○ EXCH (*IP Address*)
○ Other Hostname or IP Address
Enter the resolvable hostname or IP of the restore location.

Method: ○ Restore normally
● Restore to an Exchange Recovery Storage Group / Database
○ Restore to file system:
C:\Exchange_Restore_[redacted]\
Choose a method by which this data should be restored.

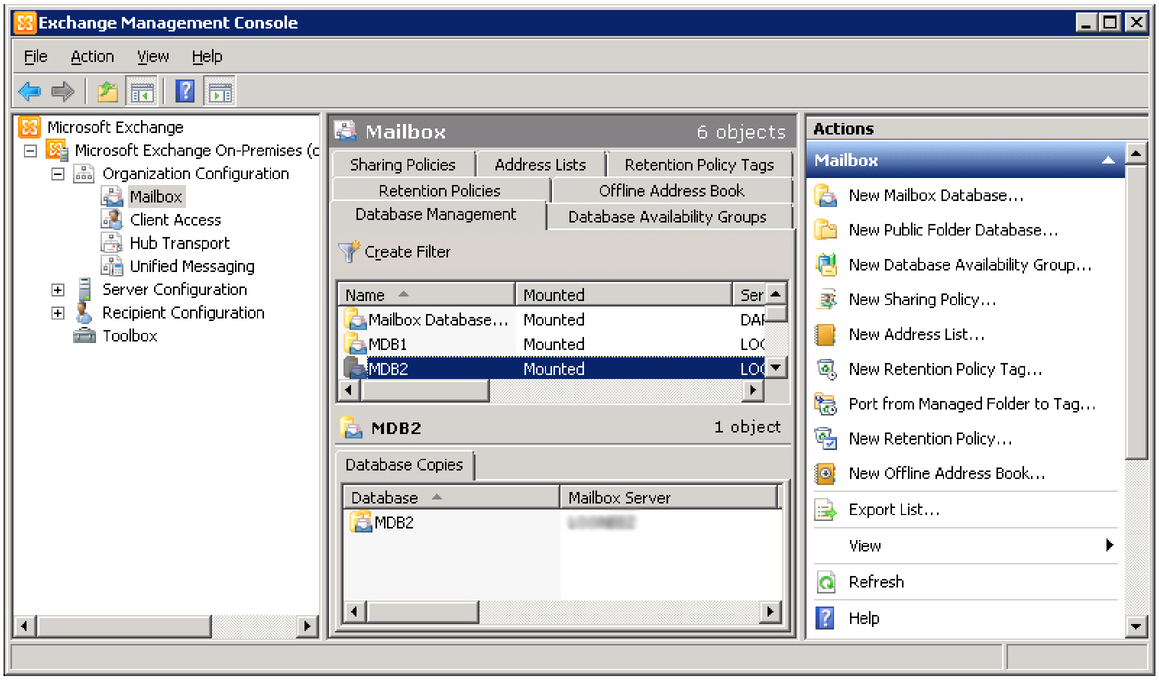
Warning: Restoring these items will overwrite any current data in the selected location.

5. Click **Start Restore**. Once the restore is complete, go to **REPORTS > Restore** to verify the restore completed successfully.

> Each Exchange 2010 server can only have ONE recovery database. Restoring again to the same server will overwrite any existing recovery databases.

Step 2. Microsoft Exchange 2010 Server

1. Log into the Exchange 2010 Server as the administrator, and open the Exchange Management Console (EMC) from **Start > All Programs > Microsoft Exchange Server > Exchange Management Console**.
2. In the left pane, expand **Microsoft Exchange > Microsoft Exchange On-Premises > Organization Configuration**, and click **Mailbox**:


Exchange Management Console
File
Action
View
Help
Microsoft Exchange
Microsoft Exchange On-Premises (c
Organization Configuration
Mailbox
Client Access
Hub Transport
Unified Messaging
Server Configuration
Recipient Configuration
Toolbox
Mailbox
6 objects
Sharing Policies
Address Lists
Retention Policy Tags
Retention Policies
Offline Address Book
Database Management
Database Availability Groups
Create Filter
MDB2
1 object
Database Copies
Actions
Mailbox
New Mailbox Database...
New Public Folder Database...
New Database Availability Group...
New Sharing Policy...
New Address List...
New Retention Policy Tag...
Port from Managed Folder to Tag...
New Retention Policy...
New Offline Address Book...
Export List...
View
Refresh
Help

Name	Mounted	Ser
Mailbox Database...	Mounted	DAI
MDB1	Mounted	LOC
MDB2	Mounted	LOC

Database	Mailbox Server
MDB2	[redacted]

3. In the center pane, click the restored recovery database, and in the right pane, click **Mount Database**. You can now restore individual mailboxes.

Step 3. Restore Microsoft Exchange 2010 Mailboxes

Once you mount the restored database, you can select to restore a single mailbox or all mailboxes.

ⓘ Any email or appointments newer than the restored data are not affected by the mailbox restore.

Option 1. Restore a Single Exchange 2010 Mailbox

Use the steps in this option to restore all email to a single mailbox. Note that you must complete **Step 1** and **Step 2** above before you can restore a single Exchange mailbox.

ⓘ You must have the name of the restored recovery database to complete these steps. The recovery database usually has the same name as the mailbox database appended with `-Recovery`.

1. Log into the Exchange 2010 Server as the administrator, and select to run the Exchange Management Shell as the administrator; the console opens.
2. At the prompt, type the following command, and then press **Enter**:
   `Restore-Mailbox -Identity user -RecoveryDatabase recoverydbname`

   ⓘ Where *`user`* is the name of the user account you want to restore, and *`recoverydbname`* is the name of the recovery database created by the restore job; if the name includes spaces, enclose the name with double quotes (" ").

3. Type Y and press **Enter** to confirm the restore operation. Once the operation is complete, the Exchange Management Shell prompt displays.
4. Ask the user to verify the mailbox has been restored; if confirmed, type `exit` in the shell, and then press **Enter**.
5. Once you are done restoring mailboxes, open the EMC, click the restored recovery database, and in the

right pane, click **Dismount Database**.

Option 2. Restore All Exchange 2010 Mailboxes

Use the steps in this option to restore all email to all mailboxes that exist in the restored recovery database. Note that you must complete **Step 1** and **Step 2** above before you can restore a single Exchange mailbox.

> ⓘ You must have the name of the restored recovery database to complete these steps. The recovery database usually has the same name as the mailbox database appended with `-Recovery`.

1. Log into the Exchange 2010 Server as the administrator, and select to run the Exchange Management Shell as the administrator; the console opens.

   > ⚠ **Warning**
   > This option restores email to all user accounts that exist in the recovery database.

2. At the prompt, type the following command, and then press **Enter**:
   `Get-Mailbox -Database dbname | Restore-Mailbox-RecoveryDatabase recoverydbname`

   > ⓘ Where *`dbname`* is the name of the mailbox database account to which to restore, and *`recoverydbname`* is the name of the recovery database created by the restore job; if the name includes spaces, enclose the name with double quotes (" ").

3. Type A and press **Enter** to confirm the restore operation for all users. Once the operation is complete, the Exchange Management Shell prompt displays.
4. Ask users to verify the mailboxes have been restored; if confirmed, type `exit` in the shell, and then press **Enter**.
5. Once the restore is complete, open the EMC, click the restored recovery database, and i n the right pane, click **Dismount Database.**

How to Restore a Microsoft Exchange 2007 Database

> This article refers to Barracuda Backup firmware 4.0 and higher, and Microsoft® Exchange Server 2007. This article assumes the Exchange Server is installed and set up.

You can select to restore an Exchange Server 2007 by overwriting an existing database or restoring to an original location, or restoring to a Recovery Storage Group (RSG).

In this article:

- Option 1. Overwrite an Existing Database or Restore to an Original Location
  - Step 1. Allow Database Restore
  - Step 2. Specify Barracuda Backup Restore Settings
  - Step 3. Remount the First Storage Group
- Option 2. Restore to a Recovery Storage Group
  - Step 1. Exchange Server 2007
  - Step 2. Barracuda Backup
  - Step 3. Exchange Server 2007

Option 1. Overwrite an Existing Database or Restore to an Original Location

> ⚠ **Warning**
> This option overwrites *all* existing data. If you do not want to overwrite the database, see **Restore to a Recovery Storage Group**.

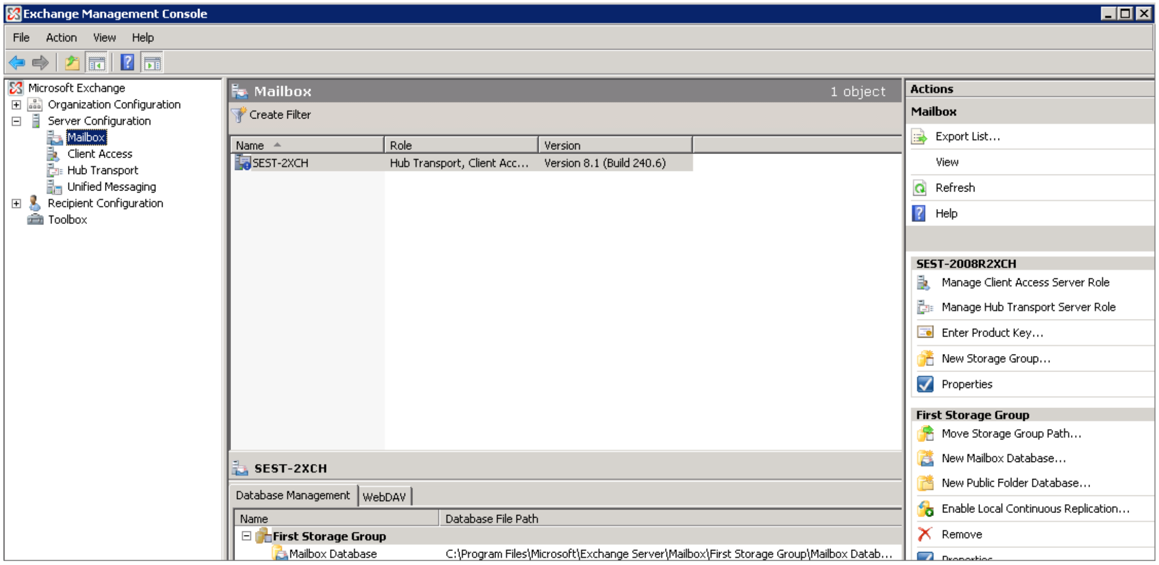
Use this option to restore by overwriting an existing database or restoring to an original location.

Click here to expand...

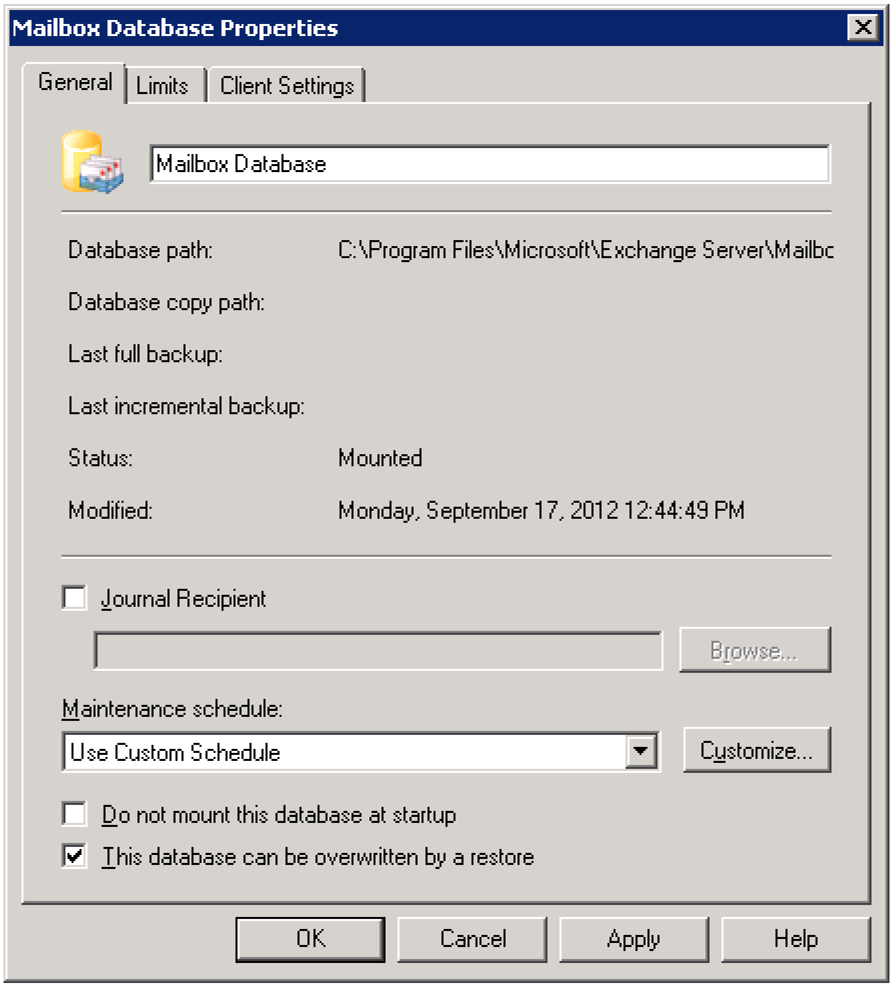
Step 1. Allow Database Restore

1. Log in to your Exchange Server as the Administrator, and open the Exchange Management Console (EMC) (**Start > All Programs > Microsoft Exchange Server > Exchange Management Console**).

2. Expand **Server Configuration**, and click **Mailbox**:


Exchange Management Console
File Action View Help
Microsoft Exchange
Organization Configuration
Server Configuration
Mailbox
Client Access
Hub Transport
Unified Messaging
Recipient Configuration
Toolbox
Mailbox
1 object
Create Filter
Name
Role
Version
SEST-2XCH
Hub Transport, Client Acc…
Version 8.1 (Build 240.6)
SEST-2XCH
Database Management
WebDAV
Name
Database File Path
First Storage Group
Mailbox Database
C:\Program Files\Microsoft\Exchange Server\Mailbox\First Storage Group\Mailbox Datab…
Actions
Mailbox
Export List…
View
Refresh
Help
SEST-2008R2XCH
Manage Client Access Server Role
Manage Hub Transport Server Role
Enter Product Key…
New Storage Group…
Properties
First Storage Group
Move Storage Group Path…
New Mailbox Database…
New Public Folder Database…
Enable Local Continuous Replication…
Remove

3. Right-click **Mailbox Database**, and click **Properties**. Select **This database can be overwritten by a restore**:


Mailbox Database Properties
General
Limits
Client Settings
Browse...
Customize...
OK
Cancel
Apply
Help

Mailbox Database

Database path: C:\Program Files\Microsoft\Exchange Server\Mailbc

Database copy path:

Last full backup:

Last incremental backup:

Status: Mounted

Modified: Monday, September 17, 2012 12:44:49 PM

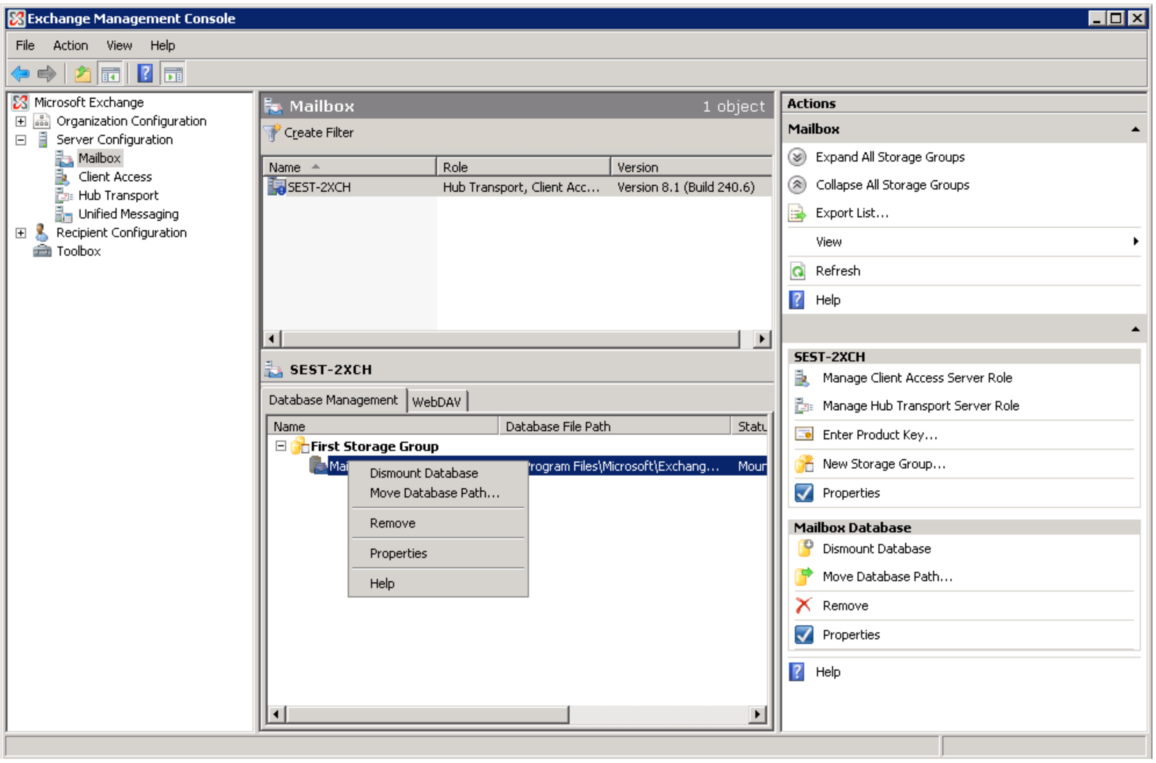
☐ Journal Recipient

Maintenance schedule: Use Custom Schedule

☐ Do not mount this database at startup

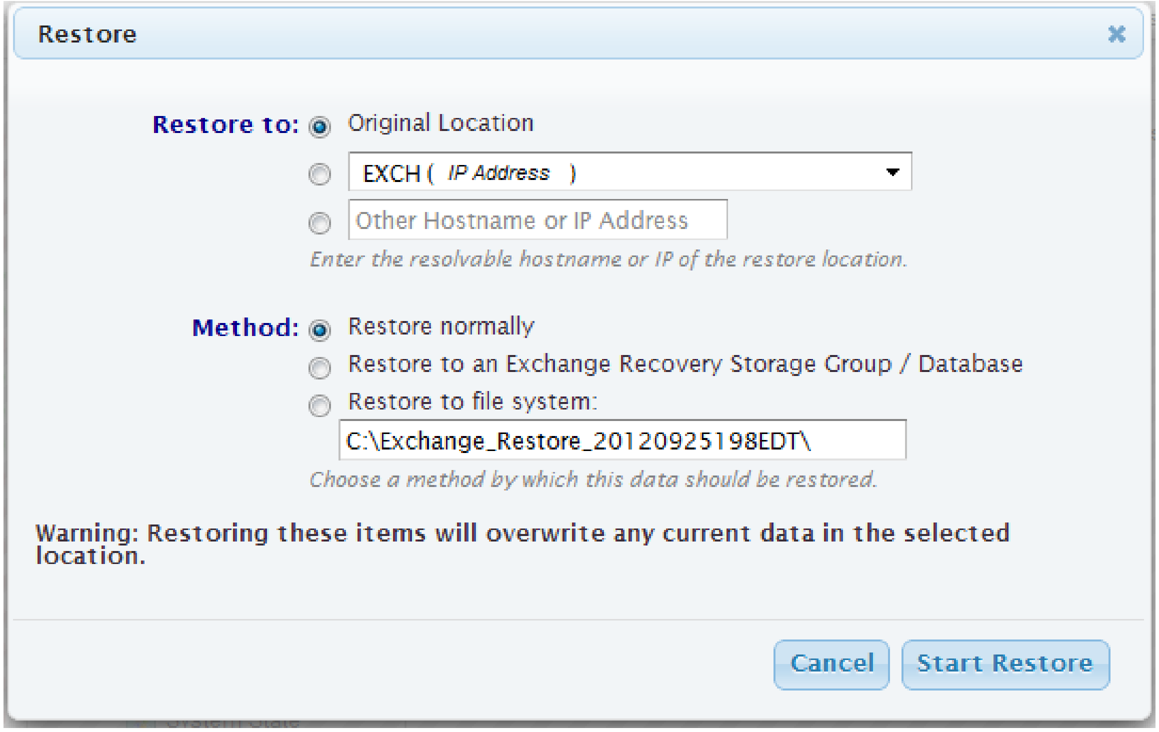
☑ This database can be overwritten by a restore

4. Click **Apply**, and **OK** to close the dialog box. Right-click the **Mailbox Database**, and click **Dismount Database**:


Exchange Management Console
File
Action
View
Help
Microsoft Exchange
Organization Configuration
Server Configuration
Mailbox
Client Access
Hub Transport
Unified Messaging
Recipient Configuration
Toolbox
Mailbox
1 object
Create Filter
Name
Role
Version
SEST-2XCH
Hub Transport, Client Acc...
Version 8.1 (Build 240.6)
SEST-2XCH
Database Management
WebDAV
Name
Database File Path
Statu
First Storage Group
Mai
rogram Files\Microsoft\Exchang...
Mour
Dismount Database
Move Database Path...
Remove
Properties
Help
Actions
Mailbox
Expand All Storage Groups
Collapse All Storage Groups
Export List...
View
Refresh
Help
SEST-2XCH
Manage Client Access Server Role
Manage Hub Transport Server Role
Enter Product Key...
New Storage Group...
Properties
Mailbox Database
Dismount Database
Move Database Path...
Remove
Properties
Help

Step 2. Specify Barracuda Backup Restore Settings

1. Log in to the Barracuda Backup Service as the administrator, and go to **RESTORE > Restore Browser**.
2. Locate the Exchange Server 2007, and navigate to the **First Storage Group**. Click **Restore**. In the **Restore** dialog box, choose the **Restore to** location:
    - Original Location
    - Select an IP Address from available servers
    - Enter an IP Address or FQDN


Restore
Cancel
Start Restore

Restore to: ● Original Location
○ EXCH (*IP Address*)
○ Other Hostname or IP Address
Enter the resolvable hostname or IP of the restore location.

Method: ● Restore normally
○ Restore to an Exchange Recovery Storage Group / Database
○ Restore to file system:
C:\Exchange_Restore_20120925198EDT\
Choose a method by which this data should be restored.

Warning: Restoring these items will overwrite any current data in the selected location.

3. Choose the Restore method as **Restore normally**, and click **Start Restore**.

Step 3. Remount the First Storage Group

Once the restore is complete, mount the database.

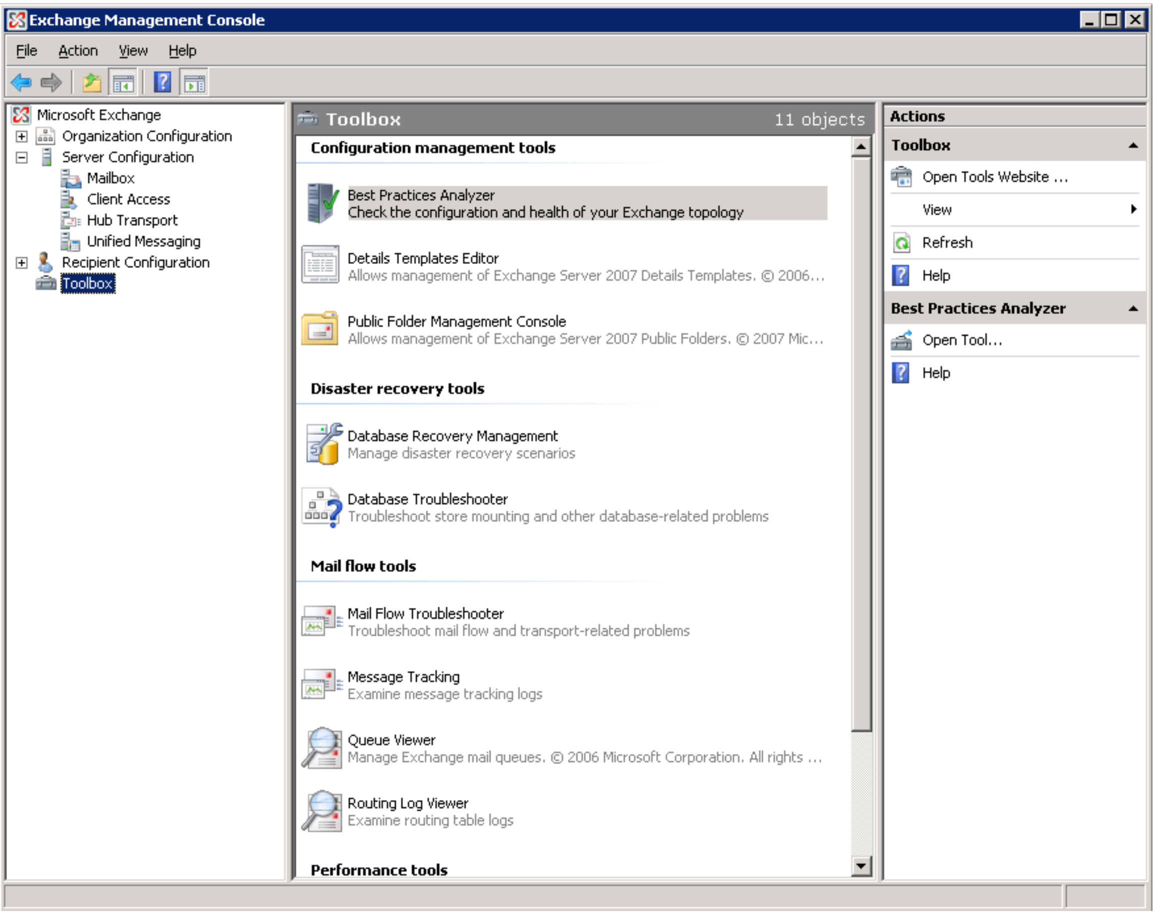
Option 2. Restore to a Recovery Storage Group

Use this option to restore to a recovery storage group (RSG).

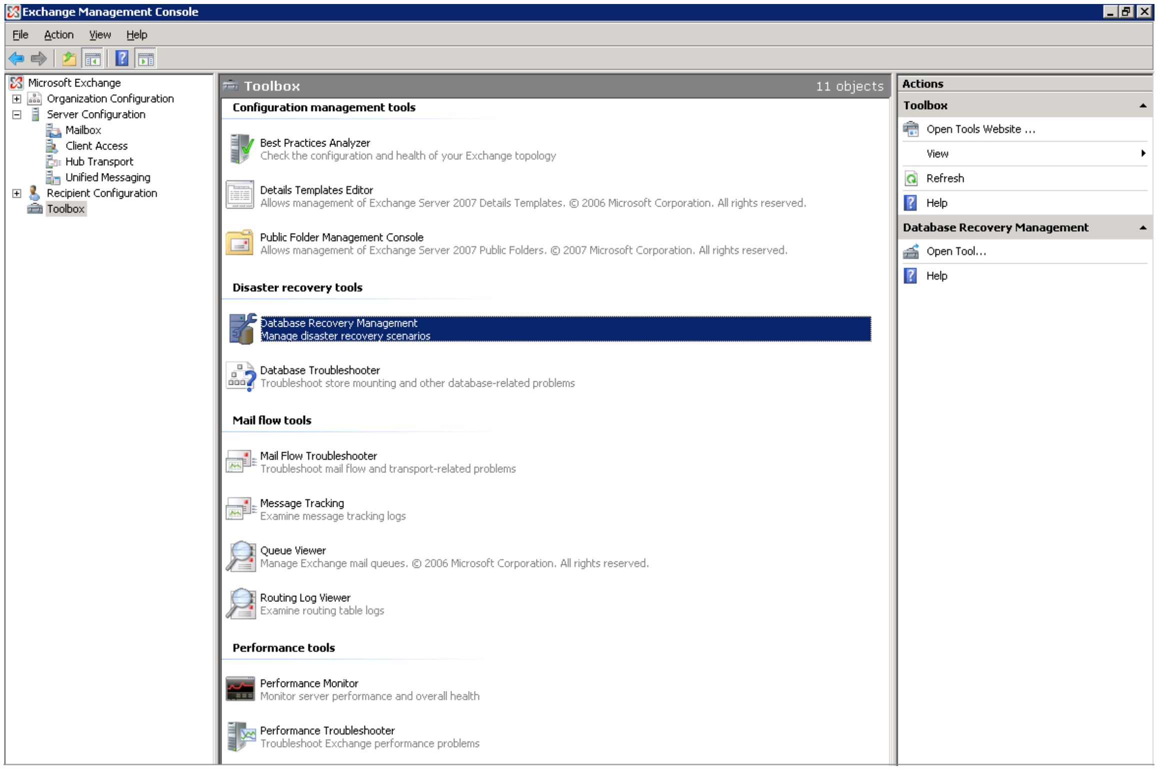
Click here to expand...

Step 1. Exchange Server 2007

1. In the EMC on the Exchange Server 2007, click **Toolbox**:


Exchange Management Console
File
Action
View
Help
Microsoft Exchange
Organization Configuration
Server Configuration
Mailbox
Client Access
Hub Transport
Unified Messaging
Recipient Configuration
Toolbox
Toolbox
11 objects
Configuration management tools
Best Practices Analyzer
Check the configuration and health of your Exchange topology
Details Templates Editor
Allows management of Exchange Server 2007 Details Templates. © 2006...
Public Folder Management Console
Allows management of Exchange Server 2007 Public Folders. © 2007 Mic...
Disaster recovery tools
Database Recovery Management
Manage disaster recovery scenarios
Database Troubleshooter
Troubleshoot store mounting and other database-related problems
Mail flow tools
Mail Flow Troubleshooter
Troubleshoot mail flow and transport-related problems
Message Tracking
Examine message tracking logs
Queue Viewer
Manage Exchange mail queues. © 2006 Microsoft Corporation. All rights ...
Routing Log Viewer
Examine routing table logs
Performance tools
Actions
Toolbox
Open Tools Website ...
View
Refresh
Help
Best Practices Analyzer
Open Tool...
Help

2. In the center pane, double click **Database Recovery Management**:


Exchange Management Console
File Action View Help
Microsoft Exchange
Organization Configuration
Server Configuration
Mailbox
Client Access
Hub Transport
Unified Messaging
Recipient Configuration
Toolbox
Actions
Toolbox
Open Tools Website ...
View
Refresh
Help
Database Recovery Management
Open Tool...
Help

Toolbox 11 objects

Configuration management tools

Best Practices Analyzer
Check the configuration and health of your Exchange topology

Details Templates Editor
Allows management of Exchange Server 2007 Details Templates. © 2006 Microsoft Corporation. All rights reserved.

Public Folder Management Console
Allows management of Exchange Server 2007 Public Folders. © 2007 Microsoft Corporation. All rights reserved.

Disaster recovery tools

Database Recovery Management
Manage disaster recovery scenarios

Database Troubleshooter
Troubleshoot store mounting and other database-related problems

Mail flow tools

Mail Flow Troubleshooter
Troubleshoot mail flow and transport-related problems

Message Tracking
Examine message tracking logs

Queue Viewer
Manage Exchange mail queues. © 2006 Microsoft Corporation. All rights reserved.

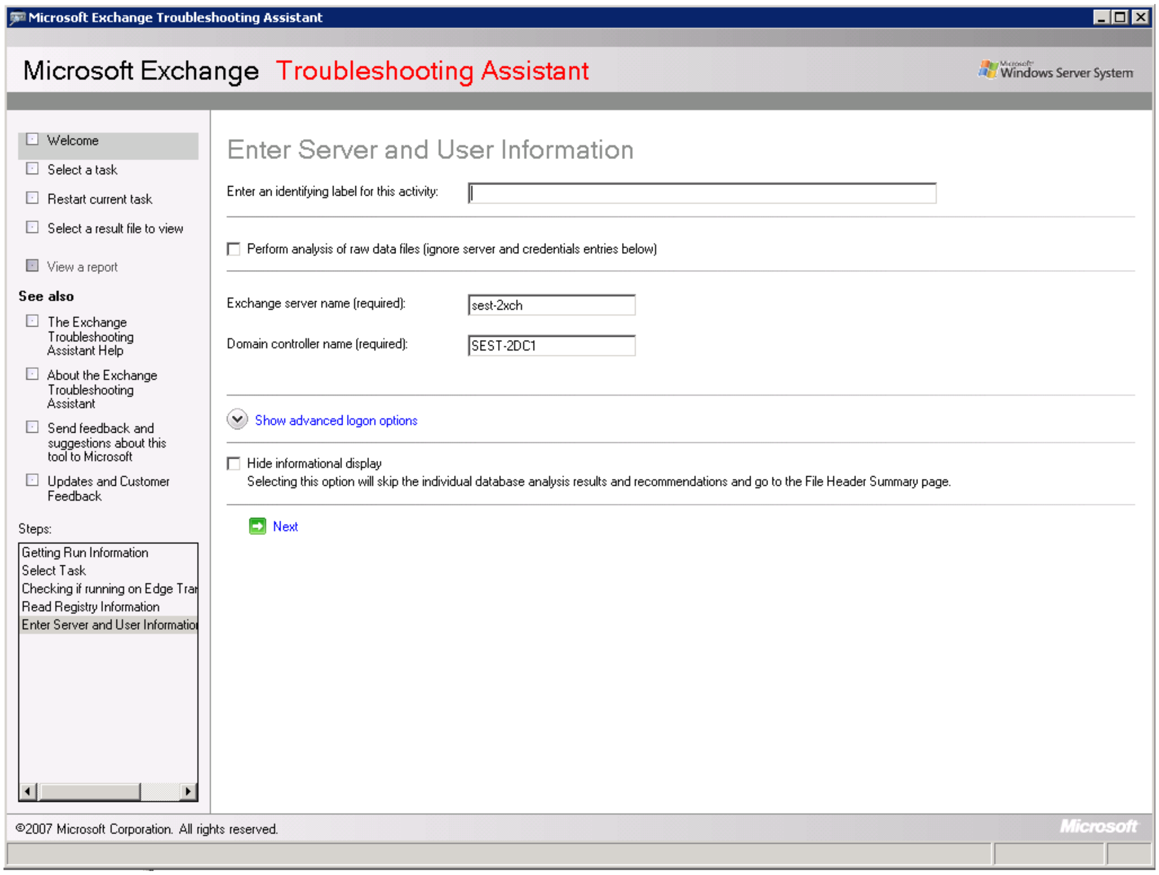
Routing Log Viewer
Examine routing table logs

Performance tools

Performance Monitor
Monitor server performance and overall health

Performance Troubleshooter
Troubleshoot Exchange performance problems

3. In the **Troubleshooting Assistant**, enter an identifying label, the Exchange server name, the Domain controller name, and click **Next**:


Microsoft Exchange Troubleshooting Assistant
Microsoft Exchange Troubleshooting Assistant
Microsoft Windows Server System
Welcome
Select a task
Restart current task
Select a result file to view
View a report
See also
The Exchange Troubleshooting Assistant Help
About the Exchange Troubleshooting Assistant
Send feedback and suggestions about this tool to Microsoft
Updates and Customer Feedback
Microsoft

Steps:
Getting Run Information
Select Task
Checking if running on Edge Tra
Read Registry Information
Enter Server and User Informatio

Enter Server and User Information

Enter an identifying label for this activity:

☐ Perform analysis of raw data files (ignore server and credentials entries below)

Exchange server name (required): sest-2xch

Domain controller name (required): SEST-2DC1

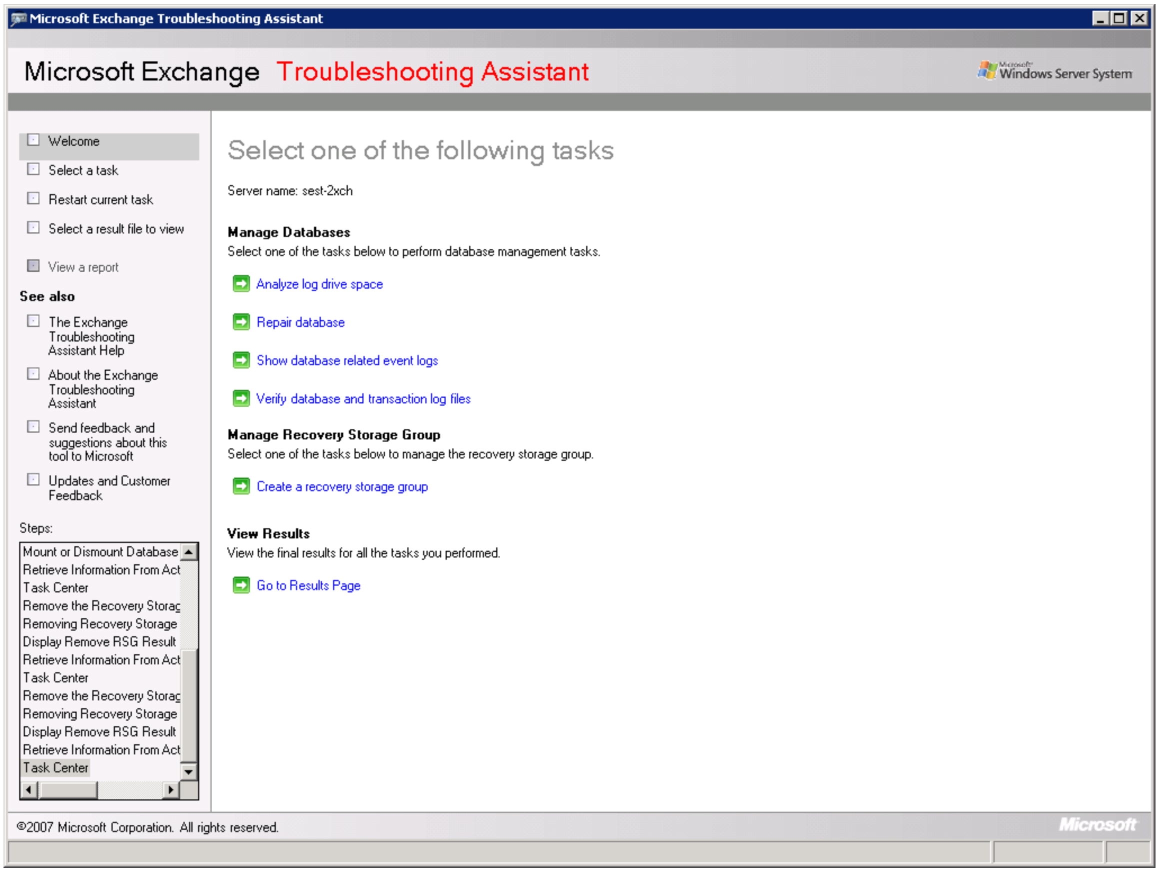
Show advanced logon options

☐ Hide informational display
Selecting this option will skip the individual database analysis results and recommendations and go to the File Header Summary page.

Next

©2007 Microsoft Corporation. All rights reserved.

4. In the next screen, click **Create a recovery storage group**, and leave the default values; Click **Create Recovery Storage Group** once again:


Microsoft Exchange Troubleshooting Assistant
Microsoft Exchange Troubleshooting Assistant
Windows Server System
Welcome
Select a task
Restart current task
Select a result file to view
View a report
See also
The Exchange Troubleshooting Assistant Help
About the Exchange Troubleshooting Assistant
Send feedback and suggestions about this tool to Microsoft
Updates and Customer Feedback
Steps:
Mount or Dismount Database
Retrieve Information From Act
Task Center
Remove the Recovery Storag
Removing Recovery Storage
Display Remove RSG Result
Retrieve Information From Act
Task Center
Remove the Recovery Storag
Removing Recovery Storage
Display Remove RSG Result
Retrieve Information From Act
Task Center
©2007 Microsoft Corporation. All rights reserved.
Microsoft

Select one of the following tasks

Server name: sest-2xch

Manage Databases

Select one of the tasks below to perform database management tasks.

- Analyze log drive space
- Repair database
- Show database related event logs
- Verify database and transaction log files

Manage Recovery Storage Group

Select one of the tasks below to manage the recovery storage group.

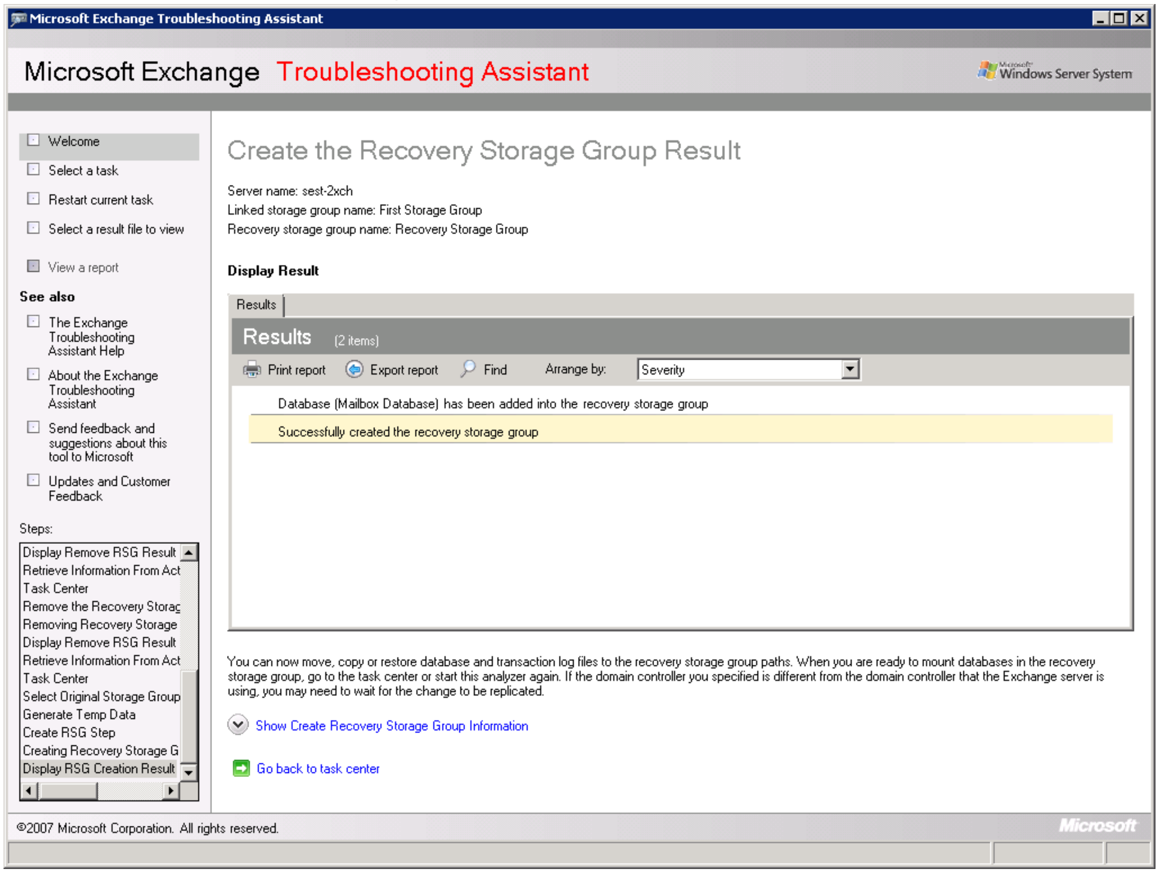
- Create a recovery storage group

View Results

View the final results for all the tasks you performed.

- Go to Results Page

5. The **Create the Recovery Storage Group Result** screen displays:


Microsoft Exchange Troubleshooting Assistant
Microsoft Exchange Troubleshooting Assistant
Windows Server System
Welcome
Select a task
Restart current task
Select a result file to view
View a report
See also
The Exchange Troubleshooting Assistant Help
About the Exchange Troubleshooting Assistant
Send feedback and suggestions about this tool to Microsoft
Updates and Customer Feedback
Steps:
Display Remove RSG Result
Retrieve Information From Act
Task Center
Remove the Recovery Storag
Removing Recovery Storage
Display Remove RSG Result
Retrieve Information From Act
Task Center
Select Original Storage Group
Generate Temp Data
Create RSG Step
Creating Recovery Storage G
Display RSG Creation Result
Results
Print report
Export report
Find
©2007 Microsoft Corporation. All rights reserved.
Microsoft

Create the Recovery Storage Group Result

Server name: sest-2xch
Linked storage group name: First Storage Group
Recovery storage group name: Recovery Storage Group

Display Result

Results (2 items)

Arrange by: Severity

Database (Mailbox Database) has been added into the recovery storage group

Successfully created the recovery storage group

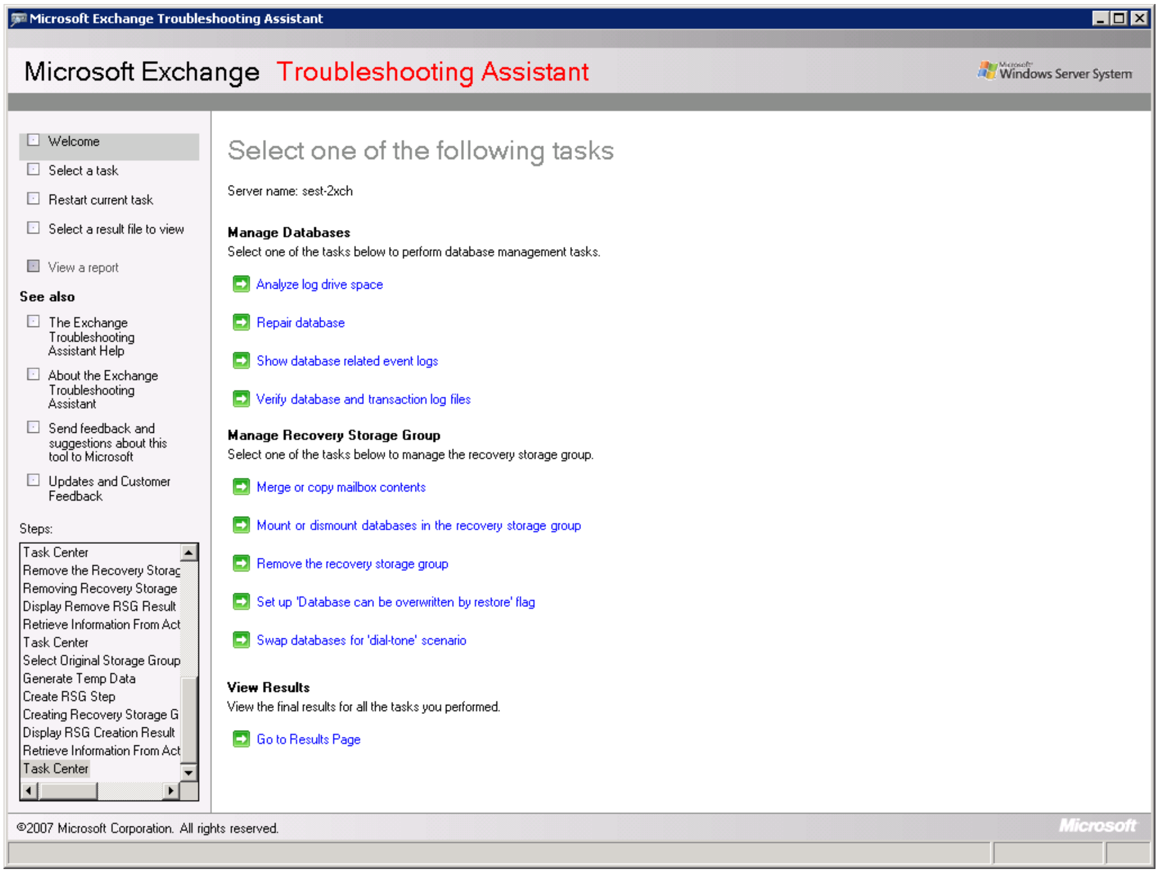
You can now move, copy or restore database and transaction log files to the recovery storage group paths. When you are ready to mount databases in the recovery storage group, go to the task center or start this analyzer again. If the domain controller you specified is different from the domain controller that the Exchange server is using, you may need to wait for the change to be replicated.

Show Create Recovery Storage Group Information

Go back to task center

6. Click **Go back to task center**. In the **Troubleshooting Assistant**, click **Set up 'Database can be**

overwritten by restore' flag:


Microsoft Exchange Troubleshooting Assistant
Microsoft Exchange Troubleshooting Assistant
Windows Server System
Welcome
Select a task
Restart current task
Select a result file to view
View a report
See also
The Exchange Troubleshooting Assistant Help
About the Exchange Troubleshooting Assistant
Send feedback and suggestions about this tool to Microsoft
Updates and Customer Feedback
Steps:
Task Center
Remove the Recovery Storag
Removing Recovery Storage
Display Remove RSG Result
Retrieve Information From Act
Task Center
Select Original Storage Group
Generate Temp Data
Create RSG Step
Creating Recovery Storage G
Display RSG Creation Result
Retrieve Information From Act
Task Center
Microsoft

Select one of the following tasks

Server name: sest-2xch

Manage Databases

Select one of the tasks below to perform database management tasks.

- Analyze log drive space
- Repair database
- Show database related event logs
- Verify database and transaction log files

Manage Recovery Storage Group

Select one of the tasks below to manage the recovery storage group.

- Merge or copy mailbox contents
- Mount or dismount databases in the recovery storage group
- Remove the recovery storage group
- Set up 'Database can be overwritten by restore' flag
- Swap databases for 'dial-tone' scenario

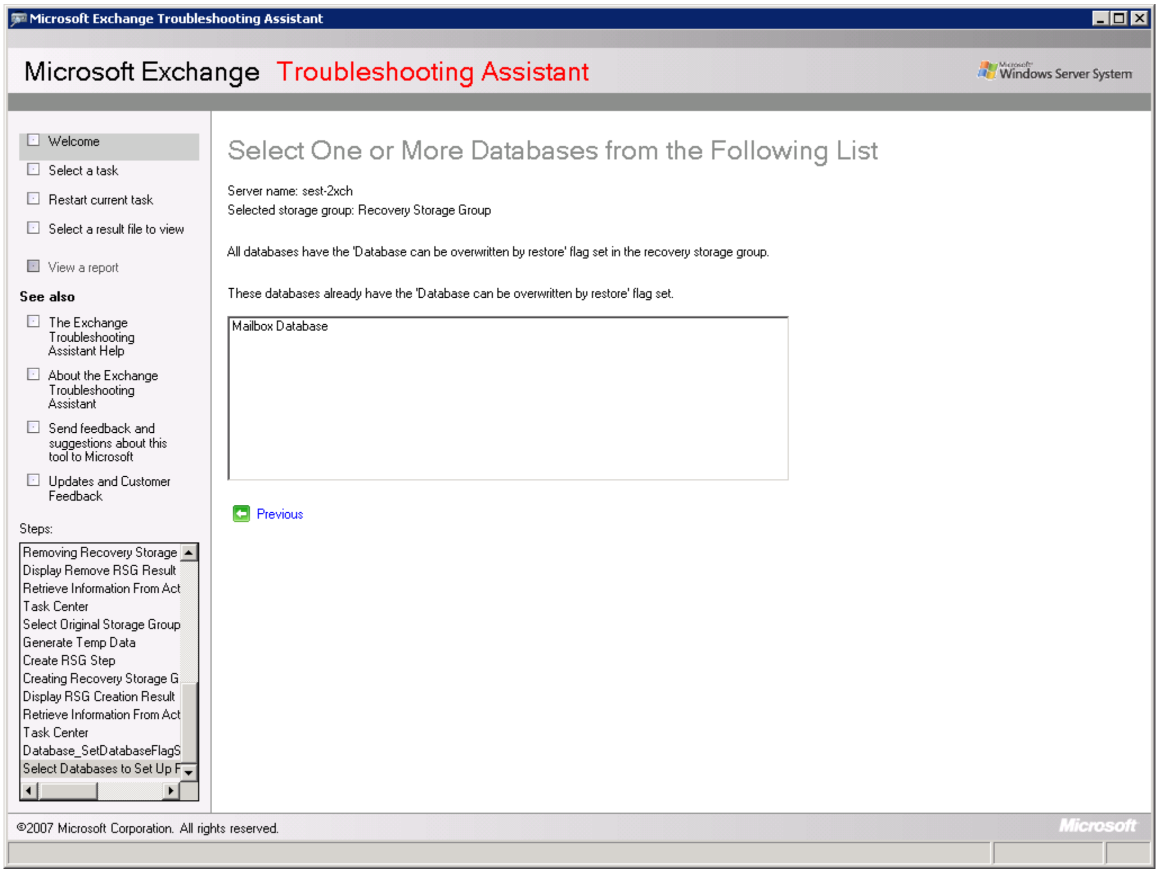
View Results

View the final results for all the tasks you performed.

- Go to Results Page

©2007 Microsoft Corporation. All rights reserved.

7. The **Databases** page displays. Verify the **Mailbox Database** displays, and click **Previous**:


Microsoft Exchange Troubleshooting Assistant
Microsoft Exchange Troubleshooting Assistant
Windows Server System
Welcome
Select a task
Restart current task
Select a result file to view
View a report
See also
The Exchange Troubleshooting Assistant Help
About the Exchange Troubleshooting Assistant
Send feedback and suggestions about this tool to Microsoft
Updates and Customer Feedback
Steps:
Removing Recovery Storage
Display Remove RSG Result
Retrieve Information From Act
Task Center
Select Original Storage Group
Generate Temp Data
Create RSG Step
Creating Recovery Storage G
Display RSG Creation Result
Retrieve Information From Act
Task Center
Database_SetDatabaseFlagS
Select Databases to Set Up F
Previous
Microsoft

Select One or More Databases from the Following List

Server name: sest-2xch

Selected storage group: Recovery Storage Group

All databases have the 'Database can be overwritten by restore' flag set in the recovery storage group.

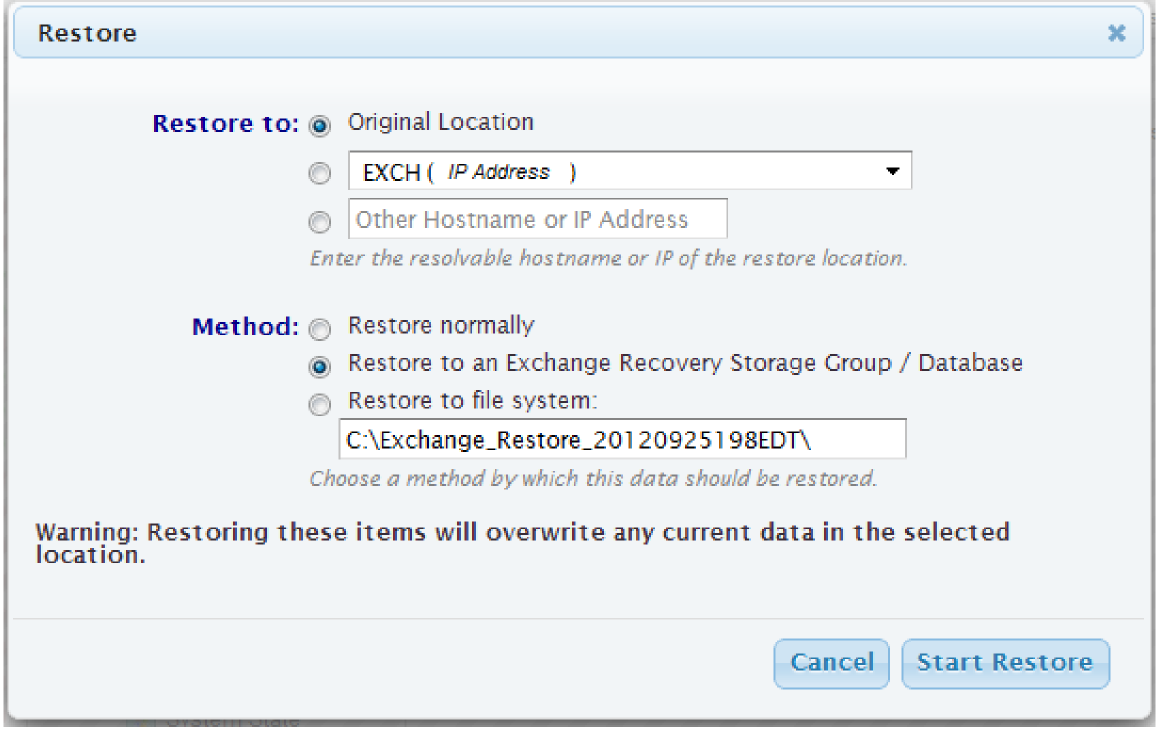
These databases already have the 'Database can be overwritten by restore' flag set.

Mailbox Database

©2007 Microsoft Corporation. All rights reserved.

Step 2. Barracuda Backup

1. In Barracuda Backup, go to **RESTORE > Restore Browser**. Locate the restored Exchange Server 2007, and navigate to the First Storage Group.
2. Click **Restore**, select the **Restore to** location, and specify the **Method** as **Restore to an Exchange Recovery Storage Group / Database**:



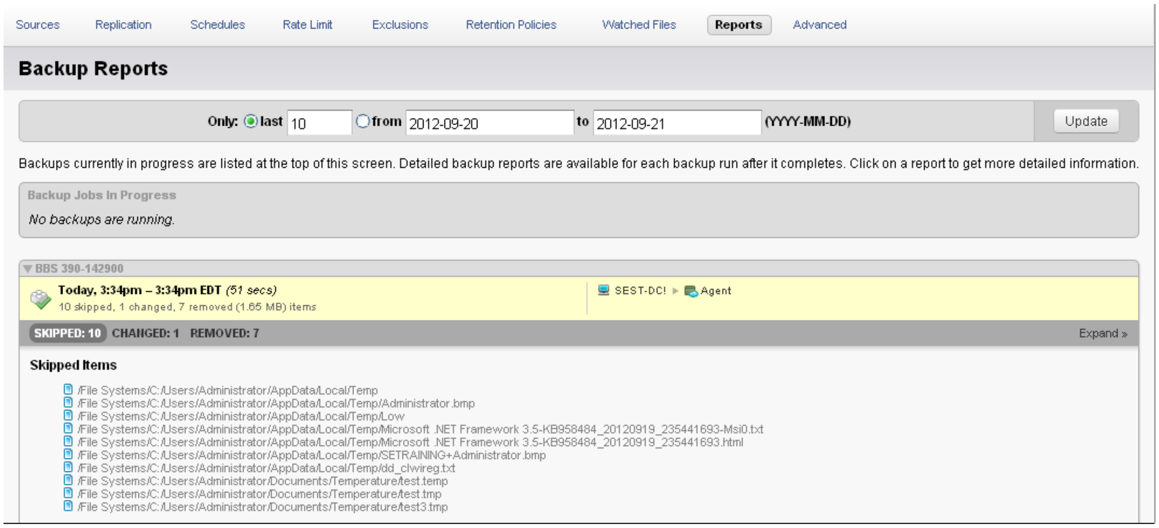
Restore

Restore to: ● Original Location
○ EXCH (*IP Address*)
○ Other Hostname or IP Address
Enter the resolvable hostname or IP of the restore location.

Method: ○ Restore normally
● Restore to an Exchange Recovery Storage Group / Database
○ Restore to file system:
C:\Exchange_Restore_20120925198EDT\
Choose a method by which this data should be restored.

Warning: Restoring these items will overwrite any current data in the selected location.

3. Click **Start Restore**. Once the restore is complete, go to **RESTORE > Restore Reports** to verify the restore completed successfully:



Backup Reports

Only: ● **last** 10 ○ **from** 2012-09-20 **to** 2012-09-21 **(YYYY-MM-DD)**

Backups currently in progress are listed at the top of this screen. Detailed backup reports are available for each backup run after it completes. Click on a report to get more detailed information.

Backup Jobs In Progress

No backups are running.

▼ **BBS 390-142900**

Today, 3:34pm – 3:34pm EDT *(51 secs)*
10 skipped, 1 changed, 7 removed (1.65 MB) items
SEST-DC! ▸ Agent

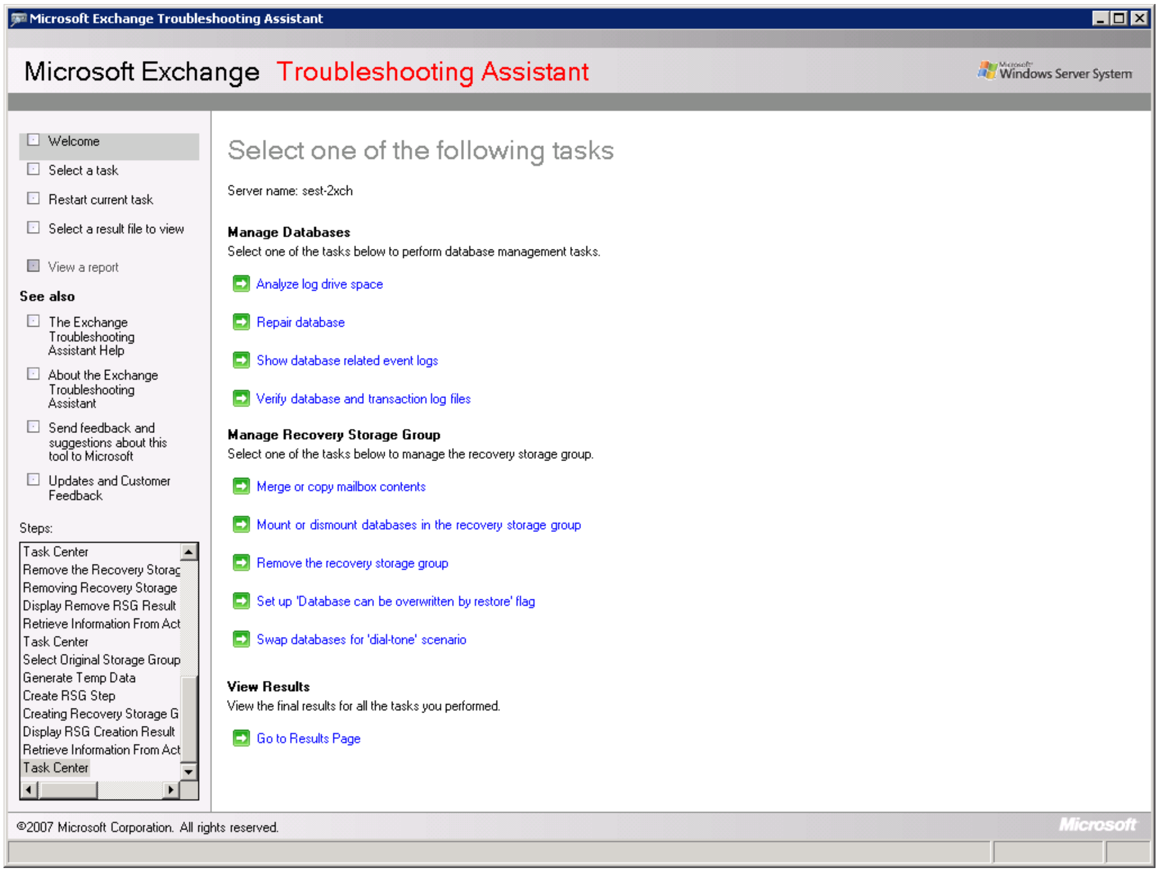
SKIPPED: 10 **CHANGED: 1** **REMOVED: 7**

Skipped Items

```
/File Systems/C:/Users/Administrator/AppData/Local/Temp
/File Systems/C:/Users/Administrator/AppData/Local/Temp/Administrator.bmp
/File Systems/C:/Users/Administrator/AppData/Local/Temp/Low
/File Systems/C:/Users/Administrator/AppData/Local/Temp/Microsoft .NET Framework 3.5-KB958484_20120919_235441693-Msi0.txt
/File Systems/C:/Users/Administrator/AppData/Local/Temp/Microsoft .NET Framework 3.5-KB958484_20120919_235441693.html
/File Systems/C:/Users/Administrator/AppData/Local/Temp/SETRAINING+Administrator.bmp
/File Systems/C:/Users/Administrator/AppData/Local/Temp/dd_clwireg.txt
/File Systems/C:/Users/Administrator/Documents/Temperature/test.temp
/File Systems/C:/Users/Administrator/Documents/Temperature/test.tmp
/File Systems/C:/Users/Administrator/Documents/Temperature/test3.tmp
```

Step 3. Exchange Server 2007

1. In the EMC on the Exchange Server 2007, in the **Troubleshooting Assistant**, click **Mount or dismount databases in the recovery storage group**:


Microsoft Exchange Troubleshooting Assistant
Microsoft Exchange Troubleshooting Assistant
Windows Server System
Welcome
Select a task
Restart current task
Select a result file to view
View a report
See also
The Exchange Troubleshooting Assistant Help
About the Exchange Troubleshooting Assistant
Send feedback and suggestions about this tool to Microsoft
Updates and Customer Feedback
Steps:
Task Center
Remove the Recovery Storag
Removing Recovery Storage
Display Remove RSG Result
Retrieve Information From Act
Task Center
Select Original Storage Group
Generate Temp Data
Create RSG Step
Creating Recovery Storage G
Display RSG Creation Result
Retrieve Information From Act
Task Center
©2007 Microsoft Corporation. All rights reserved.
Microsoft

Select one of the following tasks

Server name: sest-2xch

Manage Databases

Select one of the tasks below to perform database management tasks.

- Analyze log drive space
- Repair database
- Show database related event logs
- Verify database and transaction log files

Manage Recovery Storage Group

Select one of the tasks below to manage the recovery storage group.

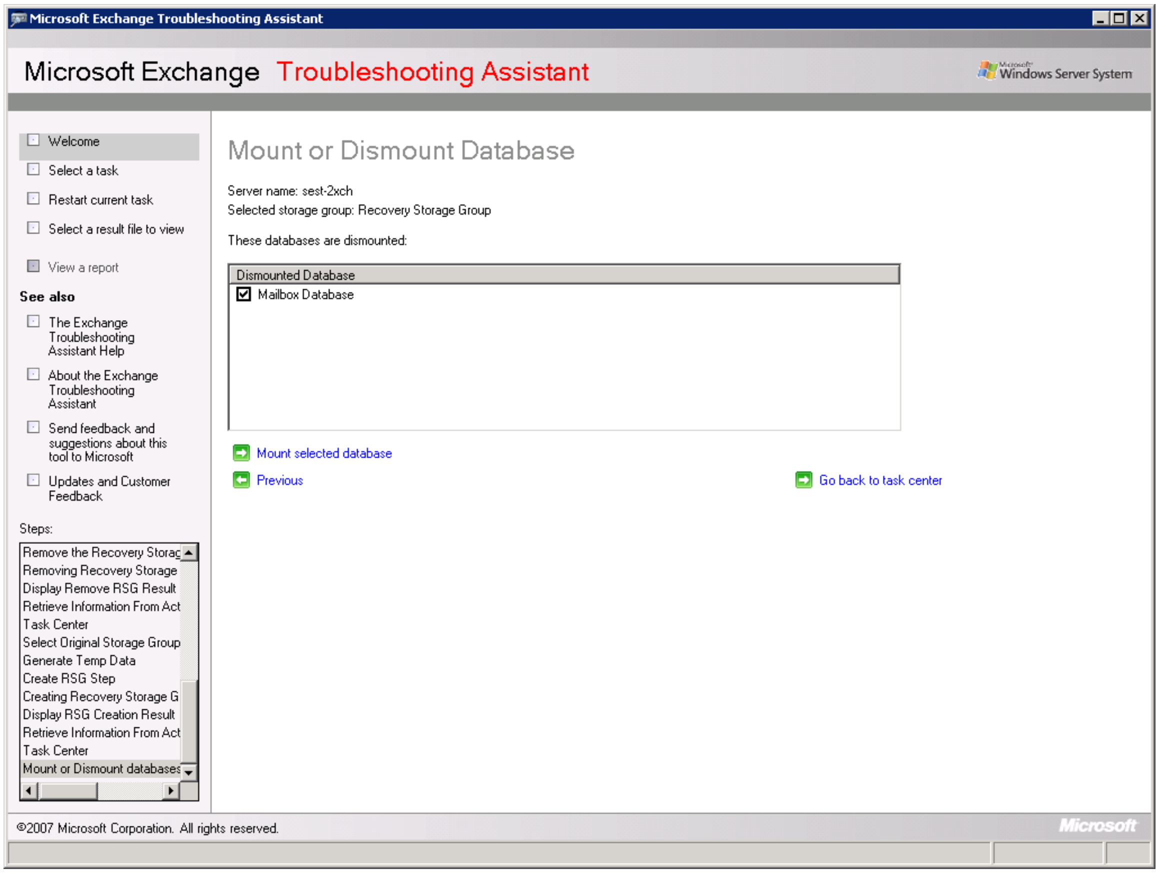
- Merge or copy mailbox contents
- Mount or dismount databases in the recovery storage group
- Remove the recovery storage group
- Set up 'Database can be overwritten by restore' flag
- Swap databases for 'dial-tone' scenario

View Results

View the final results for all the tasks you performed.

- Go to Results Page

2. Turn on **Mailbox Database**, and click **Mount selected database**:


Microsoft Exchange Troubleshooting Assistant
Microsoft Exchange Troubleshooting Assistant
Windows Server System
Welcome
Select a task
Restart current task
Select a result file to view
View a report
See also
The Exchange Troubleshooting Assistant Help
About the Exchange Troubleshooting Assistant
Send feedback and suggestions about this tool to Microsoft
Updates and Customer Feedback
Steps:
Remove the Recovery Storag
Removing Recovery Storage
Display Remove RSG Result
Retrieve Information From Act
Task Center
Select Original Storage Group
Generate Temp Data
Create RSG Step
Creating Recovery Storage G
Display RSG Creation Result
Retrieve Information From Act
Task Center
Mount or Dismount databases
Mount selected database
Previous
Go back to task center
©2007 Microsoft Corporation. All rights reserved.
Microsoft

Mount or Dismount Database

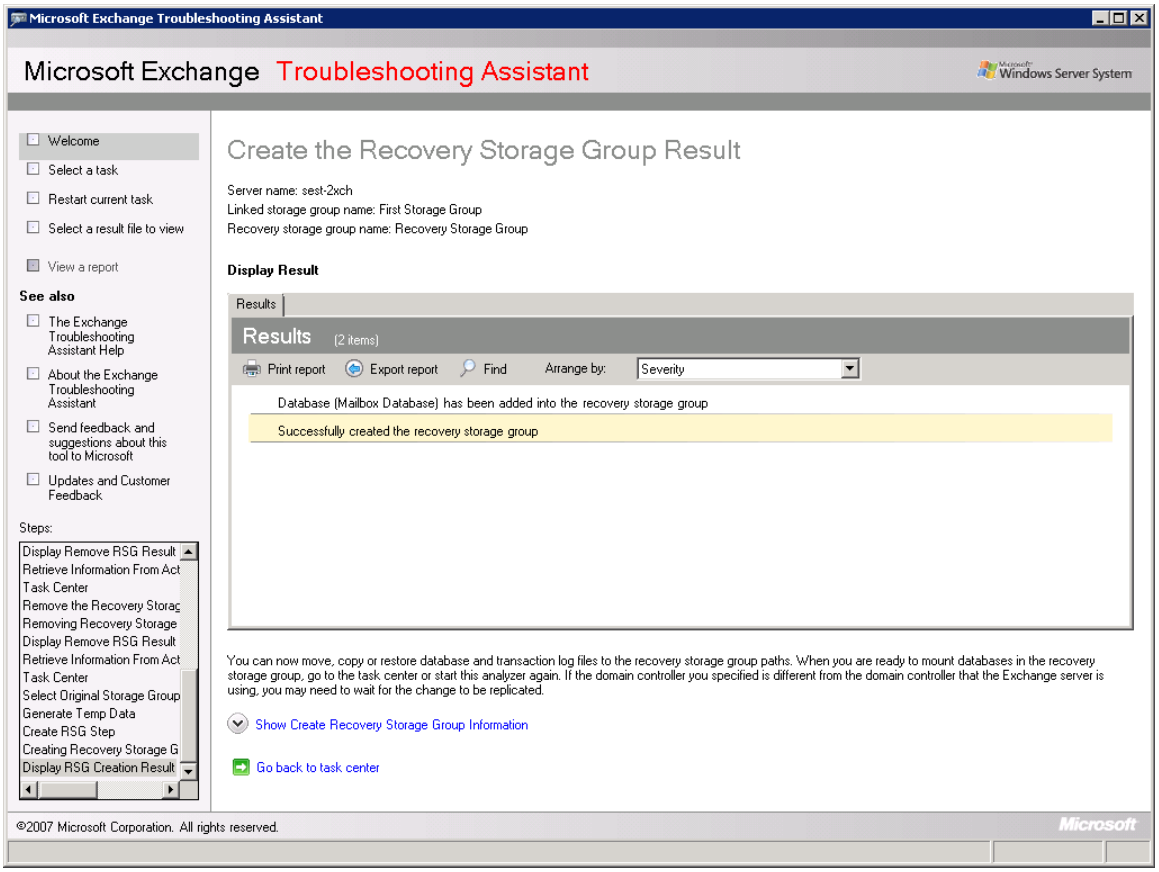
Server name: sest-2xch

Selected storage group: Recovery Storage Group

These databases are dismounted:

Dismounted Database
☑ Mailbox Database

3. The **Mount or Dismount Databases Report** displays:


Microsoft Exchange Troubleshooting Assistant
Microsoft Exchange Troubleshooting Assistant
Windows Server System
Welcome
Select a task
Restart current task
Select a result file to view
View a report
See also
The Exchange Troubleshooting Assistant Help
About the Exchange Troubleshooting Assistant
Send feedback and suggestions about this tool to Microsoft
Updates and Customer Feedback
Steps:
Display Remove RSG Result
Retrieve Information From Act
Task Center
Remove the Recovery Storag
Removing Recovery Storage
Display Remove RSG Result
Retrieve Information From Act
Task Center
Select Original Storage Group
Generate Temp Data
Create RSG Step
Creating Recovery Storage G
Display RSG Creation Result
Results
Results (2 items)
Print report
Export report
Find
Arrange by:
Severity
Microsoft

Create the Recovery Storage Group Result

Server name: sest-2xch
Linked storage group name: First Storage Group
Recovery storage group name: Recovery Storage Group

Display Result

Database (Mailbox Database) has been added into the recovery storage group

Successfully created the recovery storage group

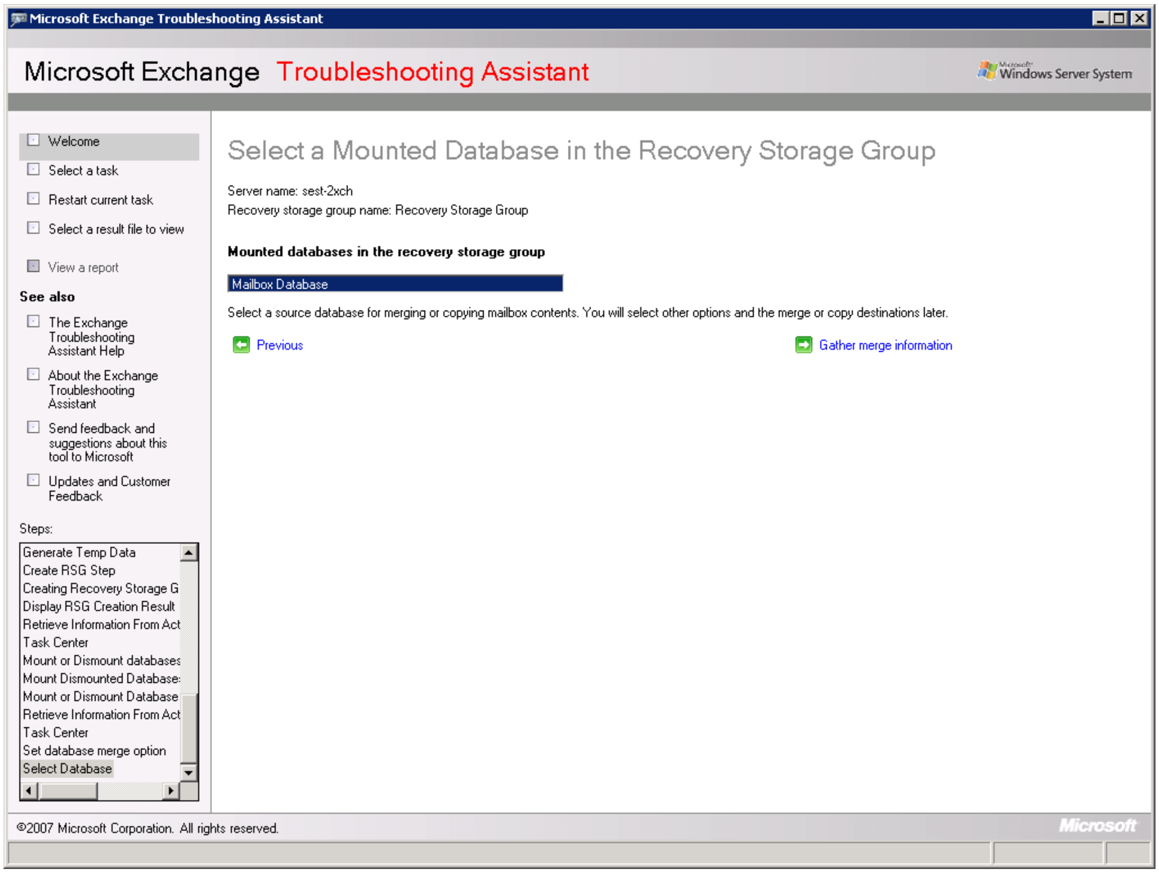
You can now move, copy or restore database and transaction log files to the recovery storage group paths. When you are ready to mount databases in the recovery storage group, go to the task center or start this analyzer again. If the domain controller you specified is different from the domain controller that the Exchange server is using, you may need to wait for the change to be replicated.

Show Create Recovery Storage Group Information

Go back to task center

©2007 Microsoft Corporation. All rights reserved.

4. Click **Go back to task center**. Click **Merge or copy mailbox contents**. Click **Gather merge information** :


Microsoft Exchange Troubleshooting Assistant
Microsoft Exchange Troubleshooting Assistant
Windows Server System
Welcome
Select a task
Restart current task
Select a result file to view
View a report
See also
The Exchange Troubleshooting Assistant Help
About the Exchange Troubleshooting Assistant
Send feedback and suggestions about this tool to Microsoft
Updates and Customer Feedback
Steps:
Generate Temp Data
Create RSG Step
Creating Recovery Storage G
Display RSG Creation Result
Retrieve Information From Act
Task Center
Mount or Dismount databases
Mount Dismounted Database:
Mount or Dismount Database
Retrieve Information From Act
Task Center
Set database merge option
Select Database
Microsoft

Select a Mounted Database in the Recovery Storage Group

Server name: sest-2xch
Recovery storage group name: Recovery Storage Group

Mounted databases in the recovery storage group

Mailbox Database

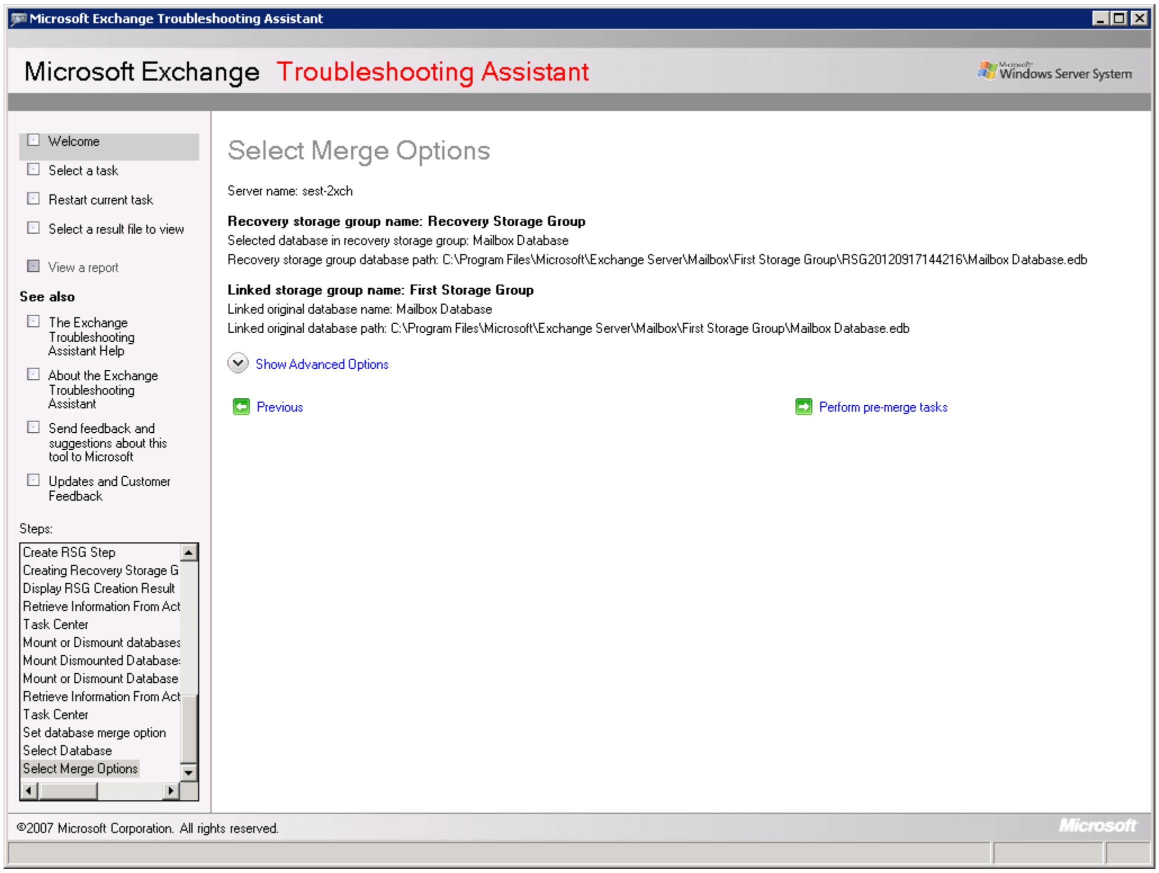
Select a source database for merging or copying mailbox contents. You will select other options and the merge or copy destinations later.

Previous

Gather merge information

©2007 Microsoft Corporation. All rights reserved.

5. Click **Perform pre-merge tasks**:


Microsoft Exchange Troubleshooting Assistant
Microsoft Exchange Troubleshooting Assistant
Windows Server System
Welcome
Select a task
Restart current task
Select a result file to view
View a report
See also
The Exchange Troubleshooting Assistant Help
About the Exchange Troubleshooting Assistant
Send feedback and suggestions about this tool to Microsoft
Updates and Customer Feedback
Steps:
Create RSG Step
Creating Recovery Storage G
Display RSG Creation Result
Retrieve Information From Act
Task Center
Mount or Dismount databases
Mount Dismounted Database
Mount or Dismount Database
Retrieve Information From Act
Task Center
Set database merge option
Select Database
Select Merge Options
Show Advanced Options
Previous
Perform pre-merge tasks
©2007 Microsoft Corporation. All rights reserved.
Microsoft

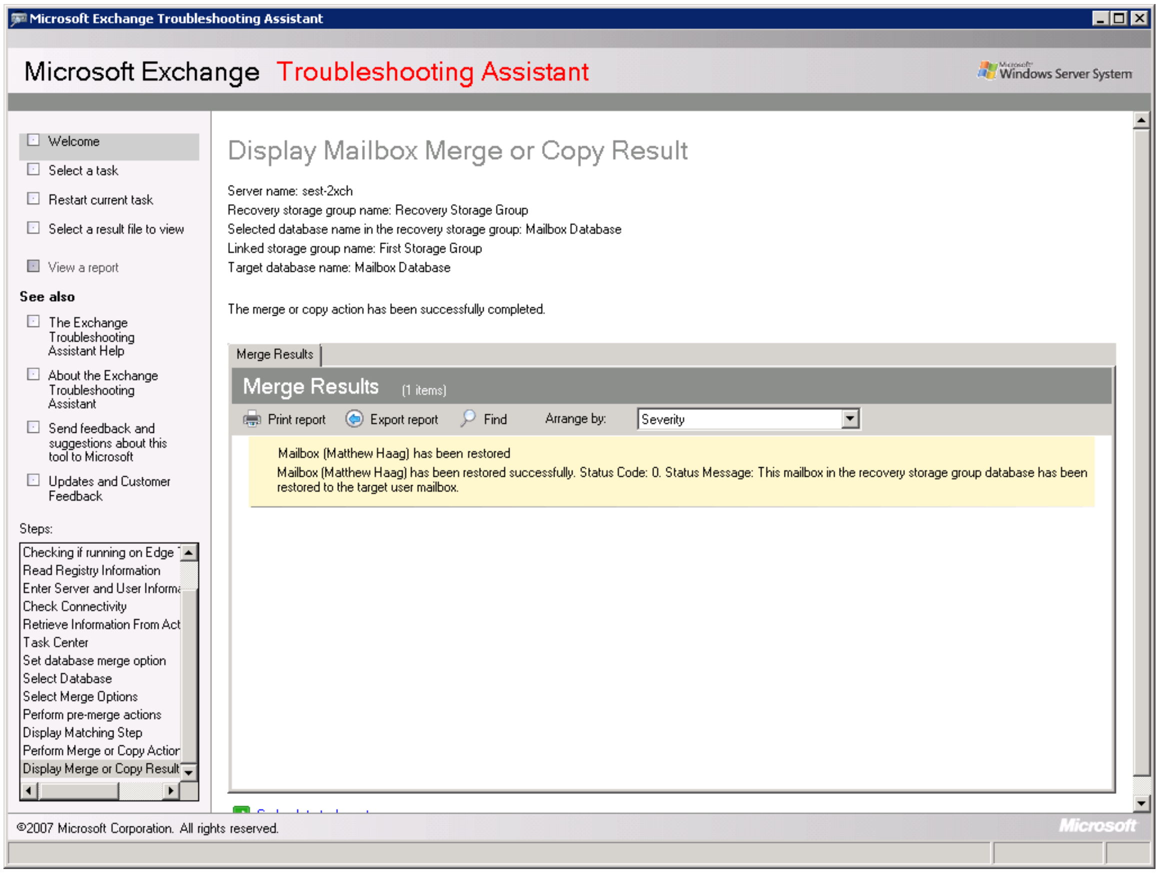
Select Merge Options

Server name: sest-2xch

Recovery storage group name: Recovery Storage Group
Selected database in recovery storage group: Mailbox Database
Recovery storage group database path: C:\Program Files\Microsoft\Exchange Server\Mailbox\First Storage Group\RSG20120917144216\Mailbox Database.edb

Linked storage group name: First Storage Group
Linked original database name: Mailbox Database
Linked original database path: C:\Program Files\Microsoft\Exchange Server\Mailbox\First Storage Group\Mailbox Database.edb

6. Turn on the mailboxes to restore, and click **Perform merge actions**; the **Results** page displays:


Microsoft Exchange Troubleshooting Assistant
Microsoft Exchange Troubleshooting Assistant
Windows Server System
Welcome
Select a task
Restart current task
Select a result file to view
View a report
See also
The Exchange Troubleshooting Assistant Help
About the Exchange Troubleshooting Assistant
Send feedback and suggestions about this tool to Microsoft
Updates and Customer Feedback
Steps:
Checking if running on Edge
Read Registry Information
Enter Server and User Informa
Check Connectivity
Retrieve Information From Act
Task Center
Set database merge option
Select Database
Select Merge Options
Perform pre-merge actions
Display Matching Step
Perform Merge or Copy Action
Display Merge or Copy Result
Merge Results
Merge Results (1 items)
Print report
Export report
Find
Arrange by:
Severity
©2007 Microsoft Corporation. All rights reserved.
Microsoft

Display Mailbox Merge or Copy Result

Server name: sest-2xch
Recovery storage group name: Recovery Storage Group
Selected database name in the recovery storage group: Mailbox Database
Linked storage group name: First Storage Group
Target database name: Mailbox Database

The merge or copy action has been successfully completed.

Mailbox (Matthew Haag) has been restored
Mailbox (Matthew Haag) has been restored successfully. Status Code: 0. Status Message: This mailbox in the recovery storage group database has been restored to the target user mailbox.

The restore is now complete.

How to Restore a Microsoft Exchange 2003 Database by Overwriting Existing Database

This article refers to all Barracuda Backup firmware versions. This article assumes you have Microsoft® Exchange 2003 installed and set up. This article describes how to restore Microsoft Exchange 2003 by either overwriting the existing database or restoring to the original location.

In this article:

- Prepare the Databases
- Dismount the Databases
- Restore the Database
- Remount the Databases

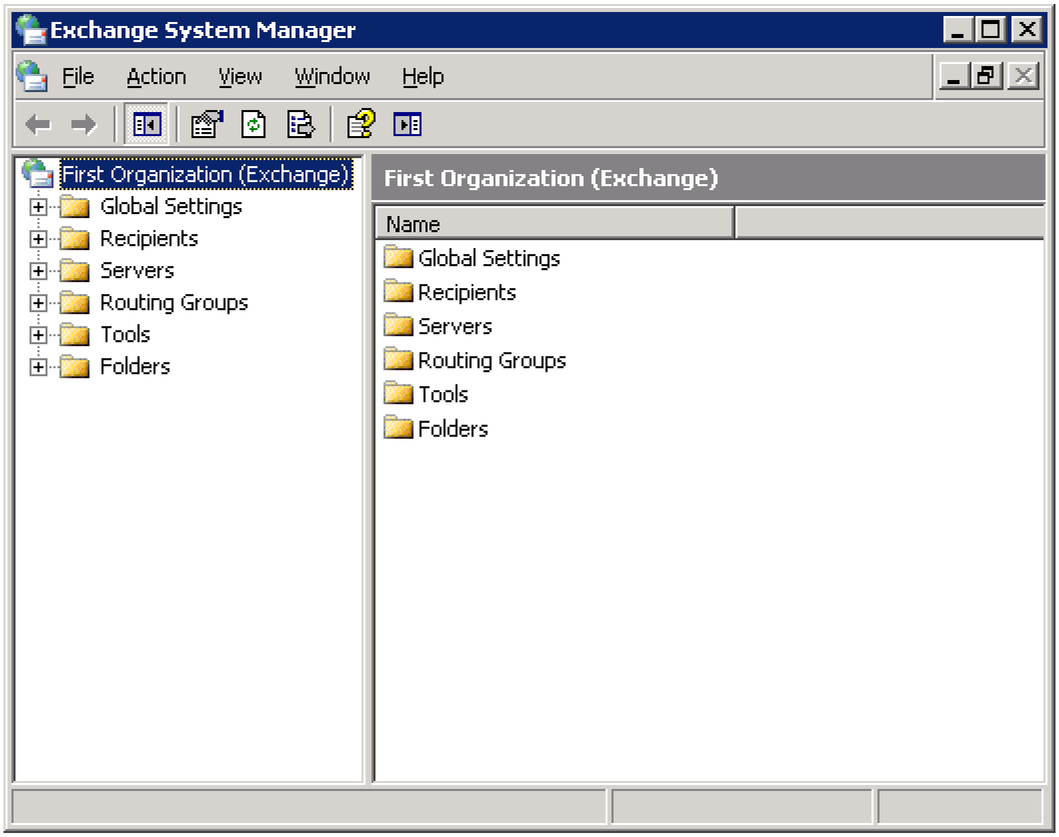
Related Articles

- Restore Using a Recovery Storage Group

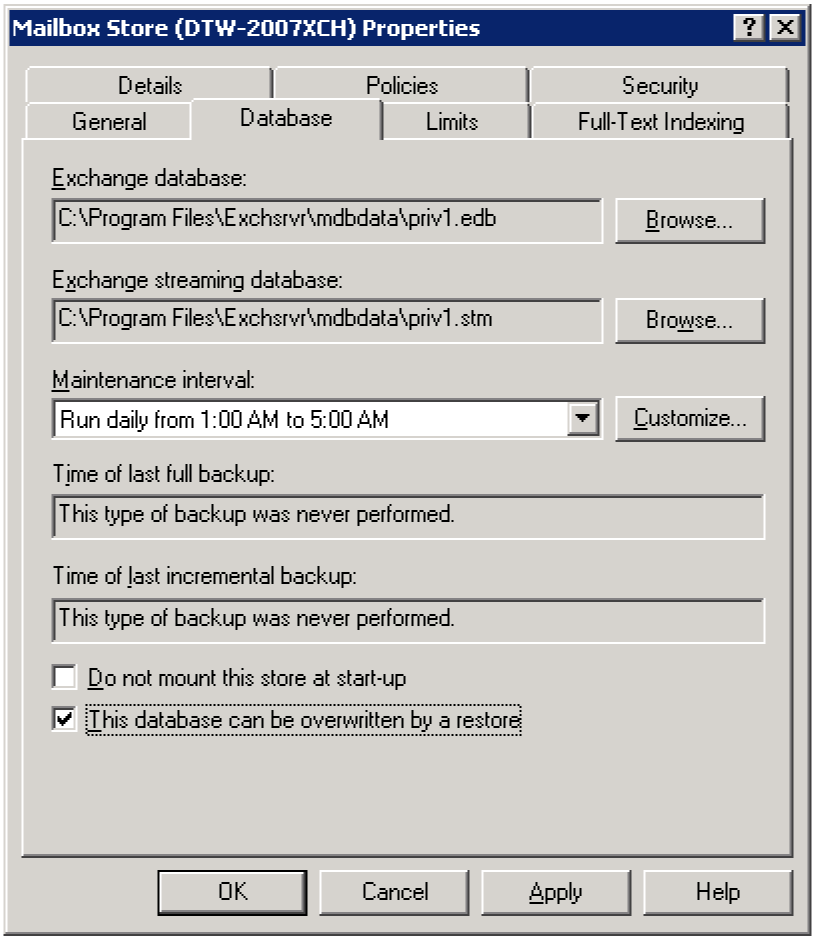
Important
Take caution when overwriting the existing database or restoring to the original location as this procedure overwrites *all* existing data. If you do not want to overwrite the existing data, you can restore the database using a Recovery Storage Group.

Prepare the Databases

1. Log into the Exchange Server as the administrator, and go to **Start > Programs > Microsoft Exchange > System Manager**:


Exchange System Manager
File
Action
View
Window
Help
First Organization (Exchange)
Global Settings
Recipients
Servers
Routing Groups
Tools
Folders
First Organization (Exchange)
Name
Global Settings
Recipients
Servers
Routing Groups
Tools
Folders

2. Expand **Administrative Groups > First Administrative Group > Servers >** *ServerName* **> First Storage Group**.
3. Right-click the **Mailbox Store**, and click **Properties**.
4. Click the **Database** tab, and select **This database can be overwritten by a restore**:


Mailbox Store (DTW-2007XCH) Properties
Details
Policies
Security
General
Database
Limits
Full-Text Indexing
Browse...
Browse...
Customize...
OK
Cancel
Apply
Help

Exchange database: C:\Program Files\Exchsrvr\mdbdata\priv1.edb

Exchange streaming database: C:\Program Files\Exchsrvr\mdbdata\priv1.stm

Maintenance interval: Run daily from 1:00 AM to 5:00 AM

Time of last full backup: This type of backup was never performed.

Time of last incremental backup: This type of backup was never performed.

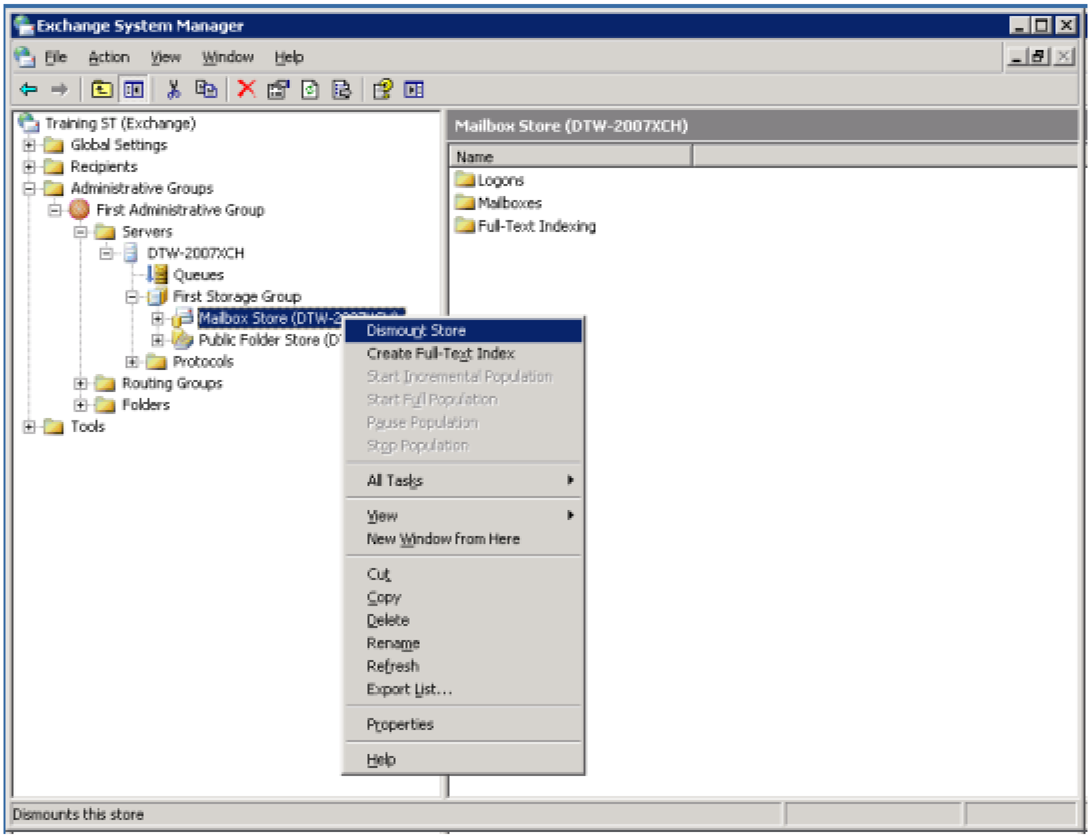
☐ Do not mount this store at start-up

☑ This database can be overwritten by a restore

5. Click **Apply**, and then click **OK**.
6. In the **System Manager**, right-click **Public Folder Store**, and click **Properties**; in the dialog box click the **Database** tab, and turn on **This database can be overwritten by a restore**.
7. Click **Apply**, and then click **OK**.

Dismount the Databases

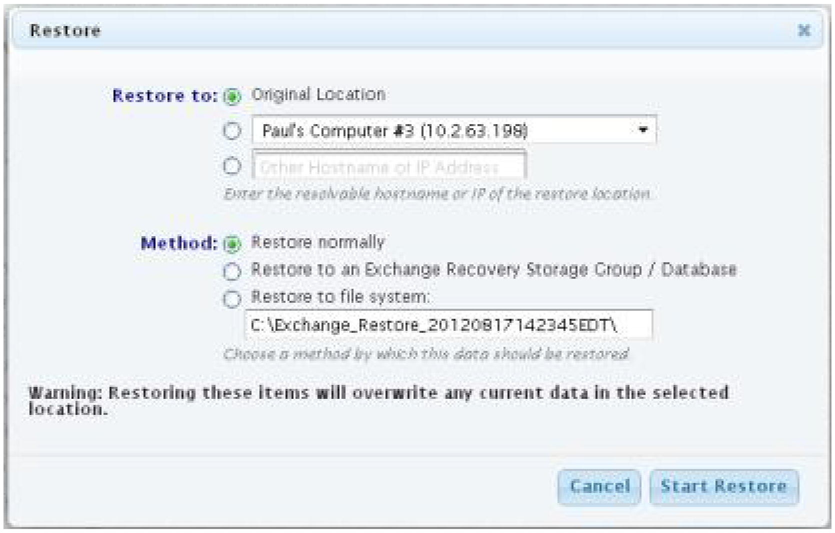
1. In the **System Manager**, right-click the **Mailbox Store**, and click **Dismount Store**:


Exchange System Manager
File Action View Window Help
Training ST (Exchange)
Global Settings
Recipients
Administrative Groups
First Administrative Group
Servers
DTW-2007XCH
Queues
First Storage Group
Mailbox Store (DTW-2007XCH)
Public Folder Store (D
Protocols
Routing Groups
Folders
Tools
Mailbox Store (DTW-2007XCH)
Name
Logons
Mailboxes
Full-Text Indexing
Dismount Store
Create Full-Text Index
Start Incremental Population
Start Full Population
Pause Population
Stop Population
All Tasks
View
New Window from Here
Cut
Copy
Delete
Rename
Refresh
Export List...
Properties
Help
Dismounts this store

2. Click **Yes** in the Warning dialog box to dismount the **Mailbox Store**.
3. In the **System Manager**, right-click the **Public Folder Store**, and click **Dismount Store**; click **Yes** in the Warning dialog box to dismount the **Public Folder Store**.

Restore the Database

1. Log into the Barracuda Backup web interface, and go to the **Restore > Restore Browser** page.
2. Expand the Microsoft Exchange 2003 Server down to the database instance to restore, and click **Restore**.
3. In the **Restore** dialog box, select the **Restore to** location where you want to restore the data, or enter a resolvable hostname or IP address of a restore location.
4. Select the **Method** as **Restore normally**, and click **Start Restore**:



Restore

Restore to: ● Original Location
○ Paul's Computer #3 (10.2.63.198)
○ Other Hostname or IP Address
Enter the resolvable hostname or IP of the restore location.

Method: ● Restore normally
○ Restore to an Exchange Recovery Storage Group / Database
○ Restore to file system:
C:\Exchange_Restore_20120817142345EDT\
Choose a method by which this data should be restored.

Warning: Restoring these items will overwrite any current data in the selected location.

Cancel
Start Restore

To view the restore status, go to the **RESTORE > Restore Reports** page, and click on a report to view individually restored items.

Remount the Databases

1. On the Exchange 2003 Server, open the **System Manager**, right-click the **Mailbox Store**, and click **Mount Store**.
2. Click **Yes** in the Warning dialog box to remount the **Mailbox Store**.
3. In the **System Manager**, right-click the **Public Folder Store**, and click **Mount Store**.
4. Click **Yes** in the Warning dialog box to remount the **Public Folder Store**.

How to Restore a Microsoft Exchange 2003 Database using a Recovery Storage Group

> This article refers to Barracuda Backup firmware version 5.0 or greater and Microsoft® Exchange 2003. This article assumes the Microsoft Exchange Server is installed and configured. This article describes how to restore Microsoft Exchange 2003 by restoring the database to a folder and using a recovery storage group to restore the database. If you do not want to use a recovery storage group, you can restore by overwriting the database.

In this article:

- Step 1. Restore Browser
- Step 2. System Manager
- Step 3. Recovery Store Group
- Step 4. Mount the Restored Database
- Step 5. Microsoft Exchange Server Mailbox Merge Wizard (ExMerge)
    - Step 5a. Extract Data from the Exchange Server Mailbox
    - Step 5b. Import Data into the Exchange Server Mailbox

Related Articles
• Restore by Overwriting Existing Database

Additional Resource
• Barracuda Networks Knowledgebase solution #00004643 • How to use Recovery Storage Groups in Exchange Server 2003

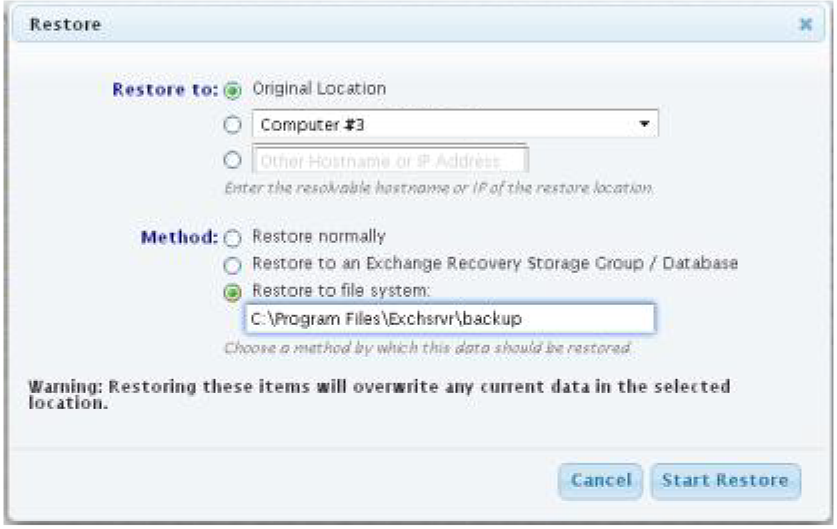
Step 1. Restore Browser

1a. Log in to the Barracuda Backup web interface, and go to the **Restore > Restore Browser** page.

1b. Expand the Microsoft Exchange 2003 Server down to the database instance you want to restore, and click **Restore**.

1c. In the **Restore** dialog box, select the **Restore to** location where you want to restore the data, or enter a resolvable hostname or IP address of a restore location.

1d. Select the **Method** as **Restore to file system**, and enter the location to which to restore, for example **C:\Program Files\Exchsrvr\backup**:



Restore

Restore to: ● Original Location

○ Computer #3

○ Other Hostname or IP Address

Enter the resolvable hostname or IP of the restore location.

Method: ○ Restore normally

○ Restore to an Exchange Recovery Storage Group / Database

● Restore to file system:

C:\Program Files\Exchsrvr\backup

Choose a method by which this data should be restored.

Warning: Restoring these items will overwrite any current data in the selected location.

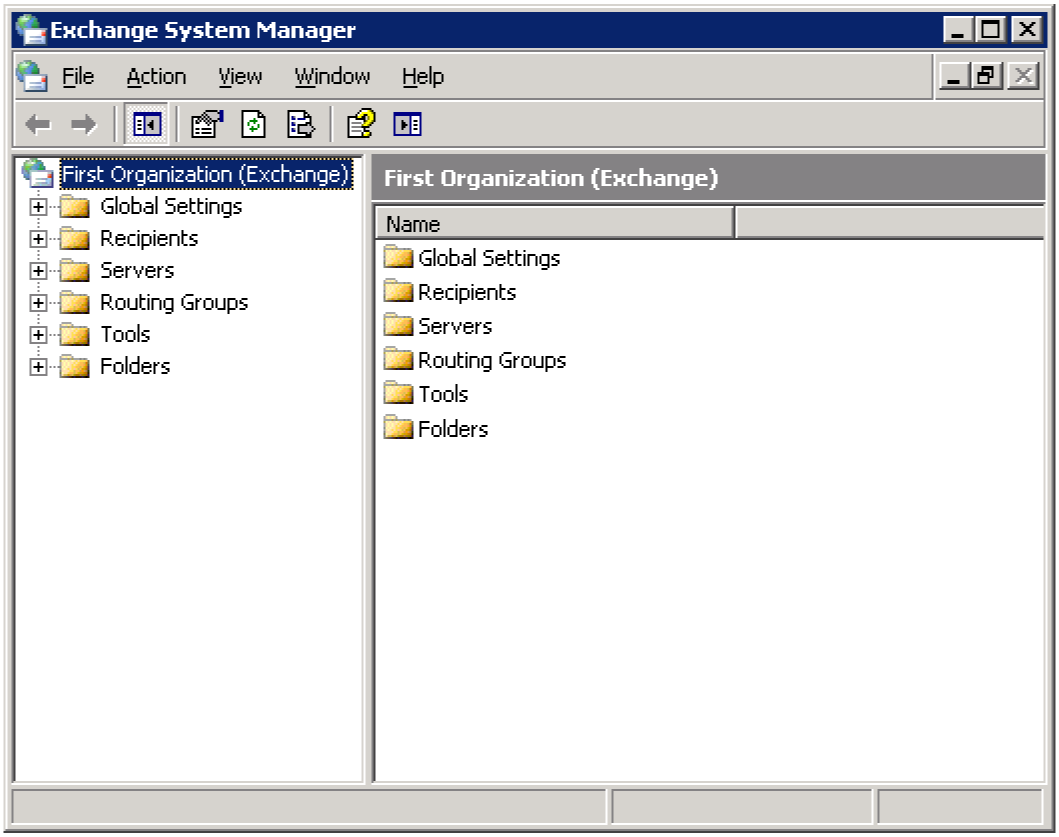
Cancel
Start Restore

1e. Click **Start Restore**.

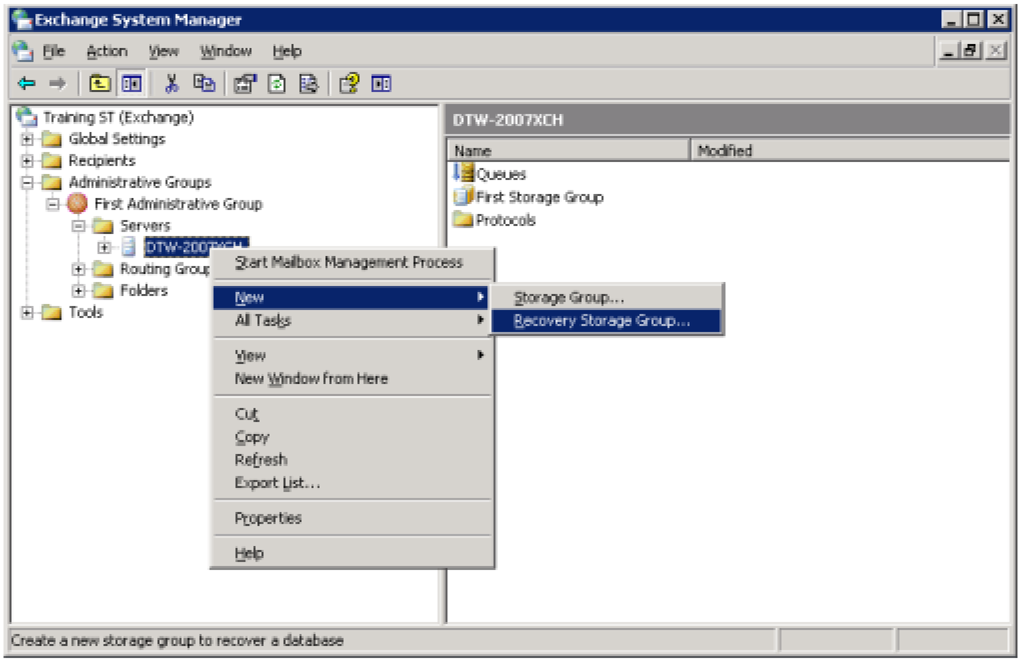
ⓘ To view the restore status, go to the **REPORTS > Restore** page, and click on a report to view individually restored items.

Step 2. System Manager

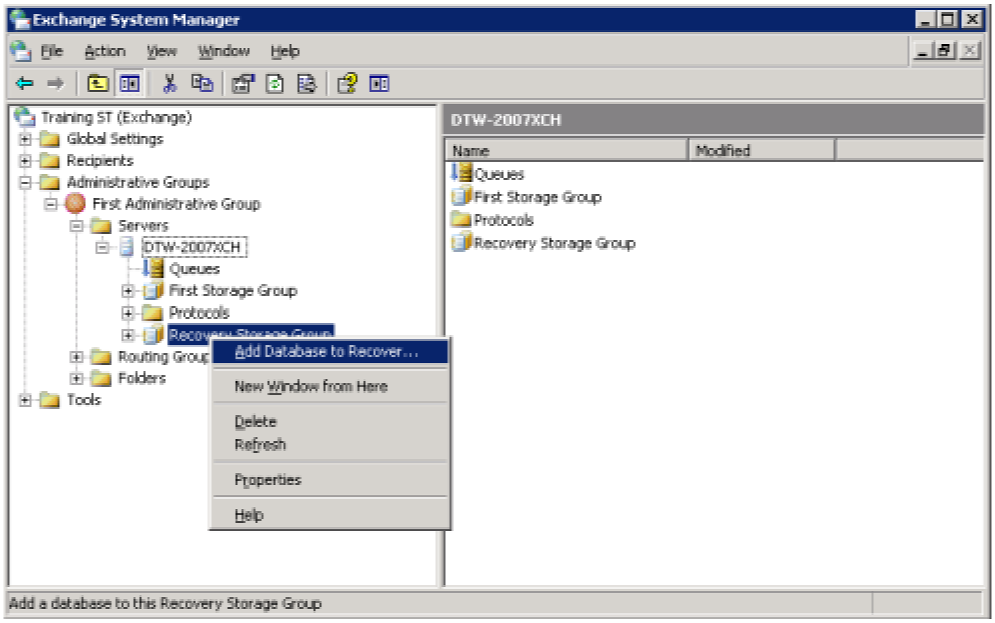
2a. Log in to the Exchange Server as the administrator, and go to **Start > Programs > Microsoft Exchange > System Manager**:


Exchange System Manager
File
Action
View
Window
Help
First Organization (Exchange)
Global Settings
Recipients
Servers
Routing Groups
Tools
Folders
First Organization (Exchange)
Name
Global Settings
Recipients
Servers
Routing Groups
Tools
Folders

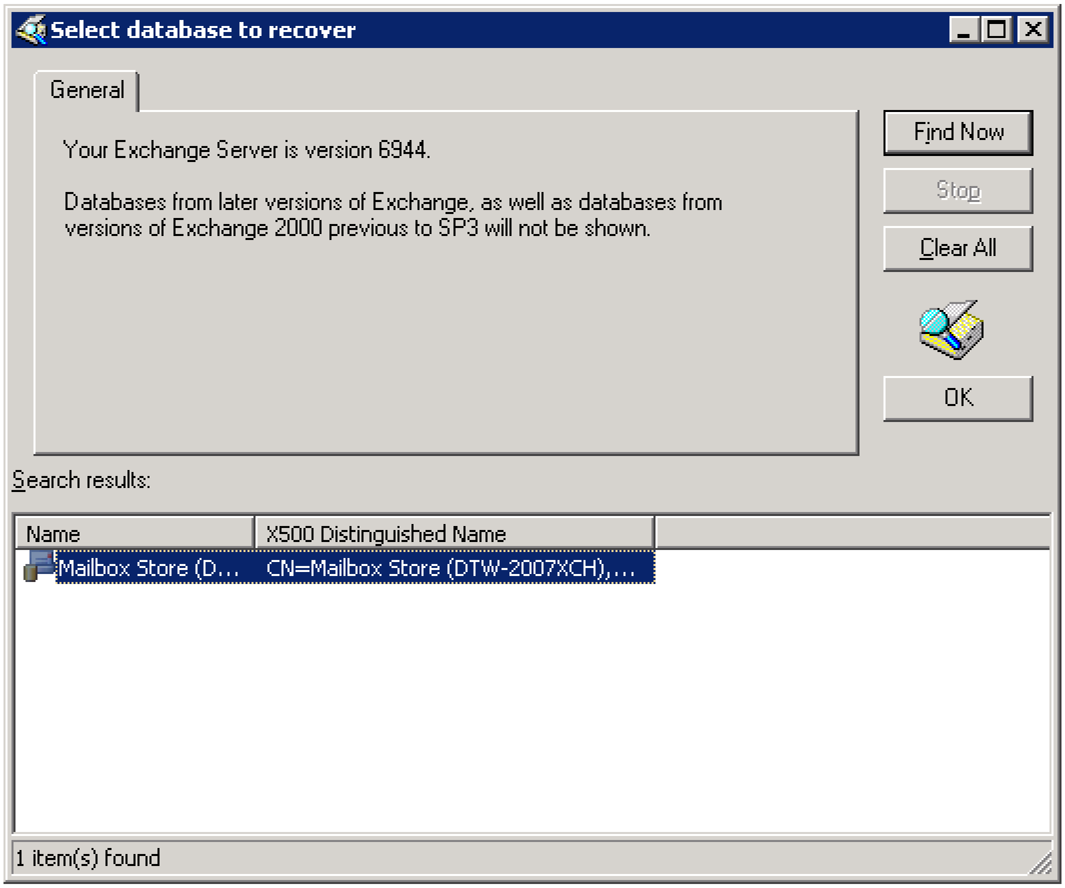
2b. Expand **Administrative Groups > First Administrative Group > Servers**, and click on your Server name. R ight-click the Server name, poin t to **New**, and click **Recovery storage Group**:


Exchange System Manager
File Action View Window Help
Training ST (Exchange)
Global Settings
Recipients
Administrative Groups
First Administrative Group
Servers
DTW-2007XCH
Routing Groups
Folders
Tools
Start Mailbox Management Process
New
All Tasks
View
New Window from Here
Cut
Copy
Refresh
Export List...
Properties
Help
Storage Group...
Recovery Storage Group...
DTW-2007XCH
Name
Modified
Queues
First Storage Group
Protocols
Create a new storage group to recover a database

2c. The **Recovery Storage Group** displays in the **System Manager**; r ight-click the **Recovery Storage Group**, and then click **Add Database to Recover**:


Exchange System Manager
File Action View Window Help
Training ST (Exchange)
Global Settings
Recipients
Administrative Groups
First Administrative Group
Servers
DTW-2007XCH
Queues
First Storage Group
Protocols
Recovery Storage Group
Routing Groups
Folders
Tools
Add Database to Recover...
New Window from Here
Delete
Refresh
Properties
Help
DTW-2007XCH
Name
Modified
Queues
First Storage Group
Protocols
Recovery Storage Group
Add a database to this Recovery Storage Group

2d. In the **Select database to recover** dialog box, select the database restore location from **Step 1d**, completed on the **RESTORE > Restore Browser** page in the Barracuda Backup web interface, and click **OK**:


Select database to recover
General
Find Now
Stop
Clear All
OK
Search results:

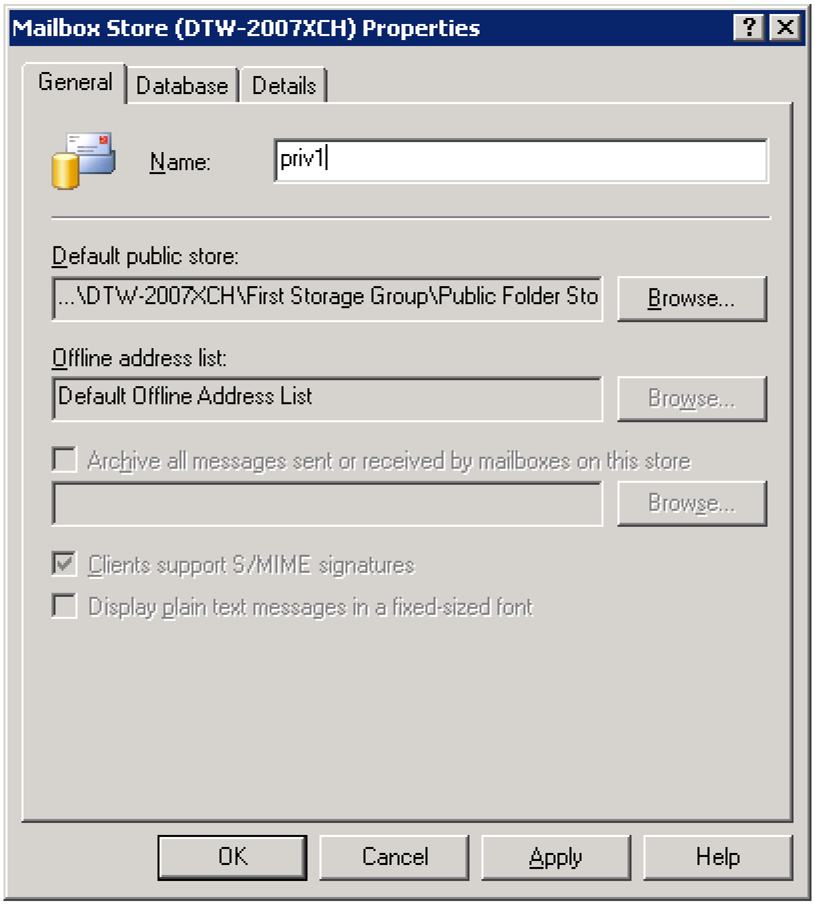
Your Exchange Server is version 6944.

Databases from later versions of Exchange, as well as databases from versions of Exchange 2000 previous to SP3 will not be shown.

Name	X500 Distinguished Name
Mailbox Store (D…	CN=Mailbox Store (DTW-2007XCH),…

1 item(s) found

2e. In the **Mailbox Store Properties** dialog box, change the value in the **Name** field, for example, **priv1**, and click **OK** to save your changes:


Mailbox Store (DTW-2007XCH) Properties
General
Database
Details
Browse...
Browse...
Browse...
OK
Cancel
Apply
Help

Name: priv1

Default public store: ...\DTW-2007XCH\First Storage Group\Public Folder Sto

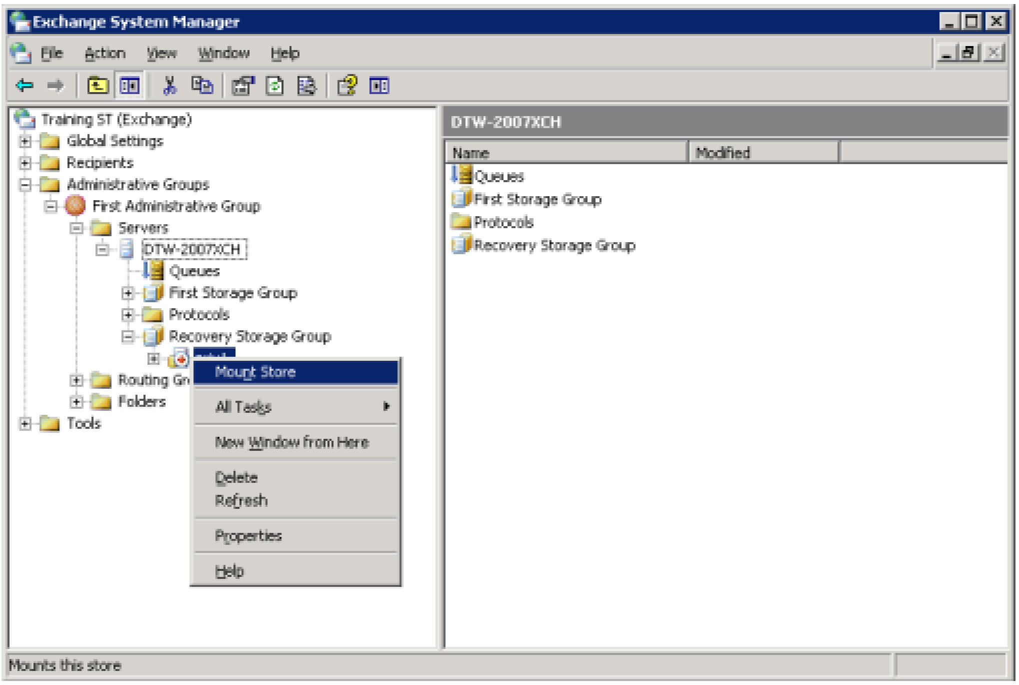
Offline address list: Default Offline Address List

☐ Archive all messages sent or received by mailboxes on this store

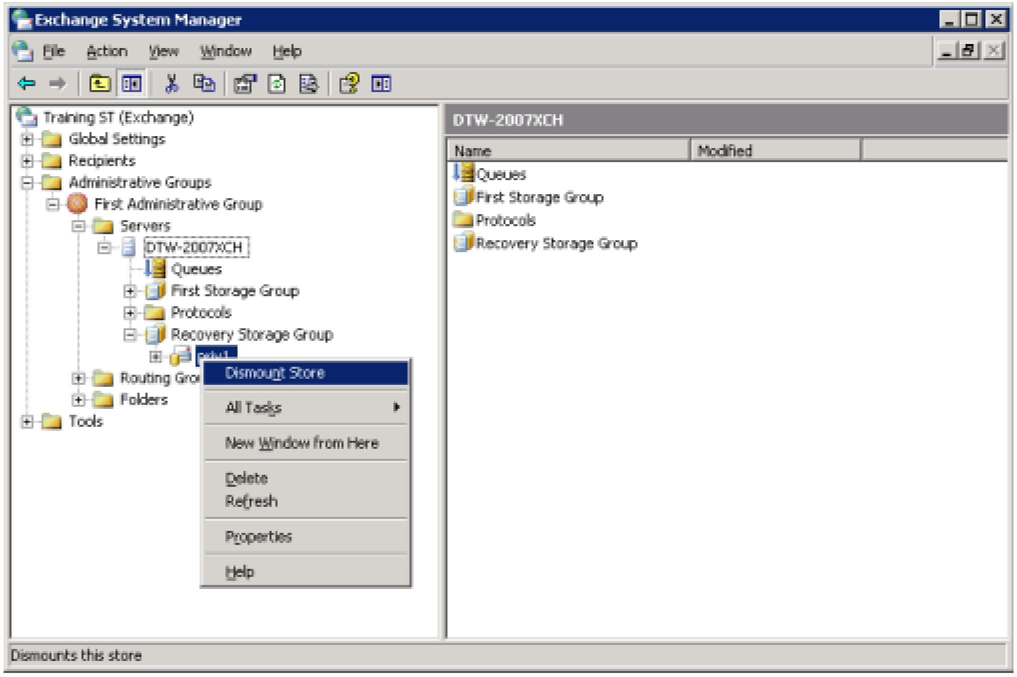
☑ Clients support S/MIME signatures

☐ Display plain text messages in a fixed-sized font

2f. In the **System Manager**, expand **Recovery storage Group**, right-click on the mailbox store **priv1** from **Step 2e**, and click **Mount Store**:


Exchange System Manager
File Action View Window Help
Training ST (Exchange)
Global Settings
Recipients
Administrative Groups
First Administrative Group
Servers
DTW-2007XCH
Queues
First Storage Group
Protocols
Recovery Storage Group
Routing Gr
Folders
Tools
Mount Store
All Tasks
New Window from Here
Delete
Refresh
Properties
Help
DTW-2007XCH
Name
Modified
Queues
First Storage Group
Protocols
Recovery Storage Group
Mounts this store

2g. Click **Yes** in the Warning dialog box. Right-click on the mailbox store **priv1** once again, and click **Dismount Store**:


Exchange System Manager
File Action View Window Help
Training ST (Exchange)
Global Settings
Recipients
Administrative Groups
First Administrative Group
Servers
DTW-2007XCH
Queues
First Storage Group
Protocols
Recovery Storage Group
Routing Gro
Folders
Tools
Dismount Store
All Tasks
New Window from Here
Delete
Refresh
Properties
Help
DTW-2007XCH
Name
Modified
Queues
First Storage Group
Protocols
Recovery Storage Group
Dismounts this store

Step 3. Recovery Store Group

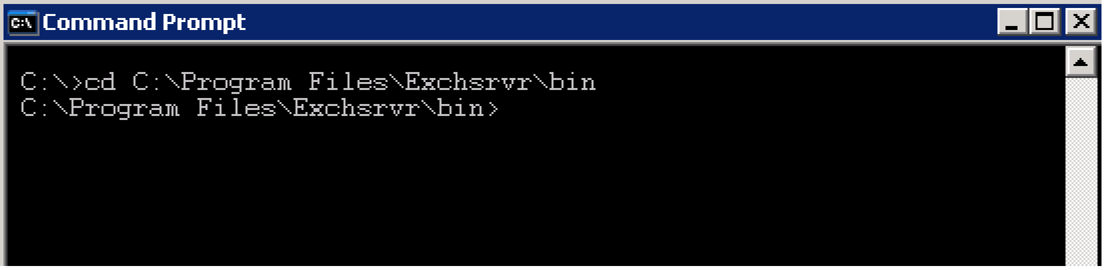
3a. On the Exchange Server in Explorer, navigate to **C:\Program Files\Exchsrvr\Recovery Storage Group**, and delete the contents of this folder.

3b. Open another window in Explorer, and navigate to the original restore location, for example, **C:\Program Files\Exchsrvr\backup**.

3c. Move the files **priv1.edb** and **priv1.stm** from the original restore location **C:\Program Files\Exchsrvr\backup** (**Step 3b**) to the **Recovery Store Group** folder (**Step 3a**).

3d. At a command prompt, enter the following command to change the directory to the original restore location:

```
cd C:\Program Files\Exchsrvr\bin
```

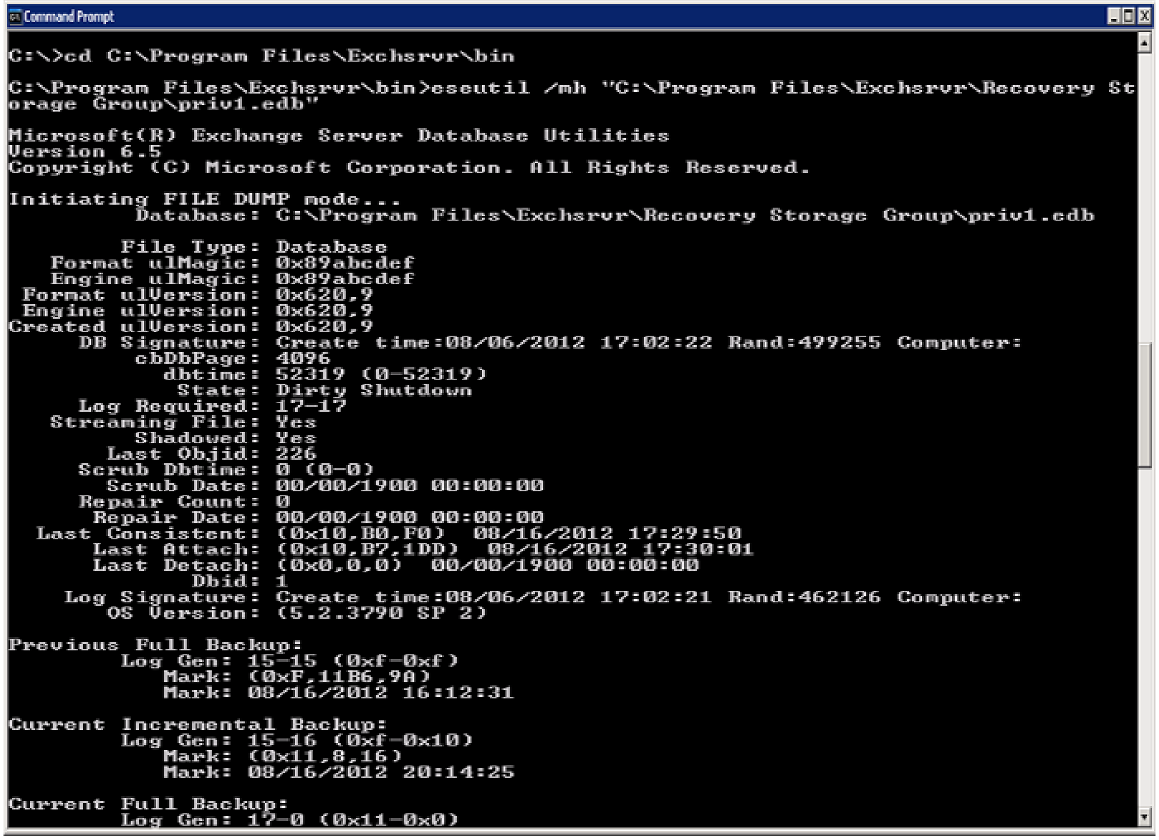


```
C:\>cd C:\Program Files\Exchsrvr\bin
C:\Program Files\Exchsrvr\bin>
```

3e. At a command prompt, enter the following command to check the database state using the Exchange tool `eseutil`:

`eseutil /mh "C:\Program Files\Exchsrvr\Recovery Storage Group\priv1.edb"`

> In this command, replace 'priv1' with the mailstore name you entered in **Step 2e**.



```
C:\>cd C:\Program Files\Exchsrvr\bin

C:\Program Files\Exchsrvr\bin>eseutil /mh "C:\Program Files\Exchsrvr\Recovery St
orage Group\priv1.edb"

Microsoft(R) Exchange Server Database Utilities
Version 6.5
Copyright (C) Microsoft Corporation. All Rights Reserved.

Initiating FILE DUMP mode...
         Database: C:\Program Files\Exchsrvr\Recovery Storage Group\priv1.edb

        File Type: Database
   Format ulMagic: 0x89abcdef
   Engine ulMagic: 0x89abcdef
 Format ulVersion: 0x620,9
 Engine ulVersion: 0x620,9
Created ulVersion: 0x620,9
     DB Signature: Create time:08/06/2012 17:02:22 Rand:499255 Computer:
         cbDbPage: 4096
           dbtime: 52319 (0-52319)
            State: Dirty Shutdown
     Log Required: 17-17
   Streaming File: Yes
         Shadowed: Yes
       Last Objid: 226
     Scrub Dbtime: 0 (0-0)
       Scrub Date: 00/00/1900 00:00:00
     Repair Count: 0
      Repair Date: 00/00/1900 00:00:00
  Last Consistent: (0x10,B0,F0)  08/16/2012 17:29:50
      Last Attach: (0x10,B7,1DD)  08/16/2012 17:30:01
      Last Detach: (0x0,0,0)  00/00/1900 00:00:00
             Dbid: 1
    Log Signature: Create time:08/06/2012 17:02:21 Rand:462126 Computer:
       OS Version: (5.2.3790 SP 2)

Previous Full Backup:
        Log Gen: 15-15 (0xf-0xf)
           Mark: (0xF,11B6,9A)
           Mark: 08/16/2012 16:12:31

Current Incremental Backup:
        Log Gen: 15-16 (0xf-0x10)
           Mark: (0x11,8,16)
           Mark: 08/16/2012 20:14:25

Current Full Backup:
        Log Gen: 17-0 (0x11-0x0)
```

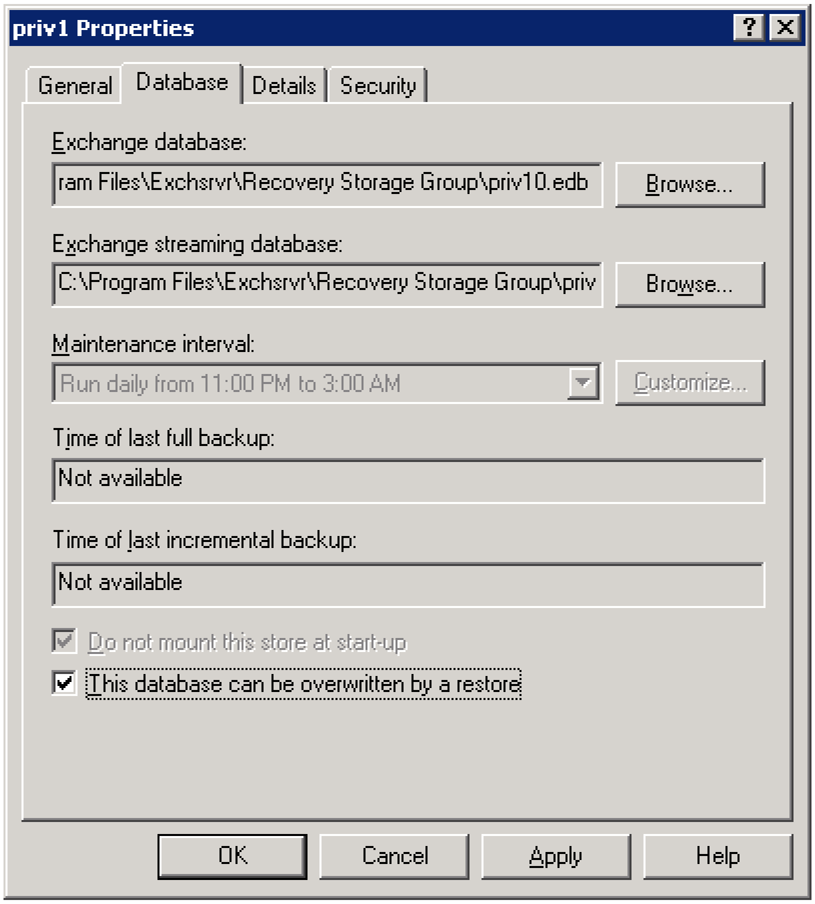
3f. If the database is in a 'Dirty Shutdown' state, at a command prompt, enter the following command:

`eseutil /p "C:\Program Files\Exchsrvr\Recovery Storage Group\priv1.edb"`

> To further repair the Exchange database, from the command prompt, run the defragment command:
> `eseutil /d "C:\Program Files\Exchsrvr\Recovery Storage Group\priv1.edb" /p`
>
> In this command, replace 'priv1' with the mailstore name you entered in **Step 2e**.

Step 4. Mount the Restored Database

4a. In the **System Manager**, right-click on the database **priv1**, and click **Properties**. Click the **Database** tab, and select **This database can be overwritten by a restore**:



Exchange database: ram Files\Exchsrvr\Recovery Storage Group\priv10.edb

Exchange streaming database: C:\Program Files\Exchsrvr\Recovery Storage Group\priv

Maintenance interval: Run daily from 11:00 PM to 3:00 AM

Time of last full backup: Not available

Time of last incremental backup: Not available

☑ Do not mount this store at start-up

☑ This database can be overwritten by a restore

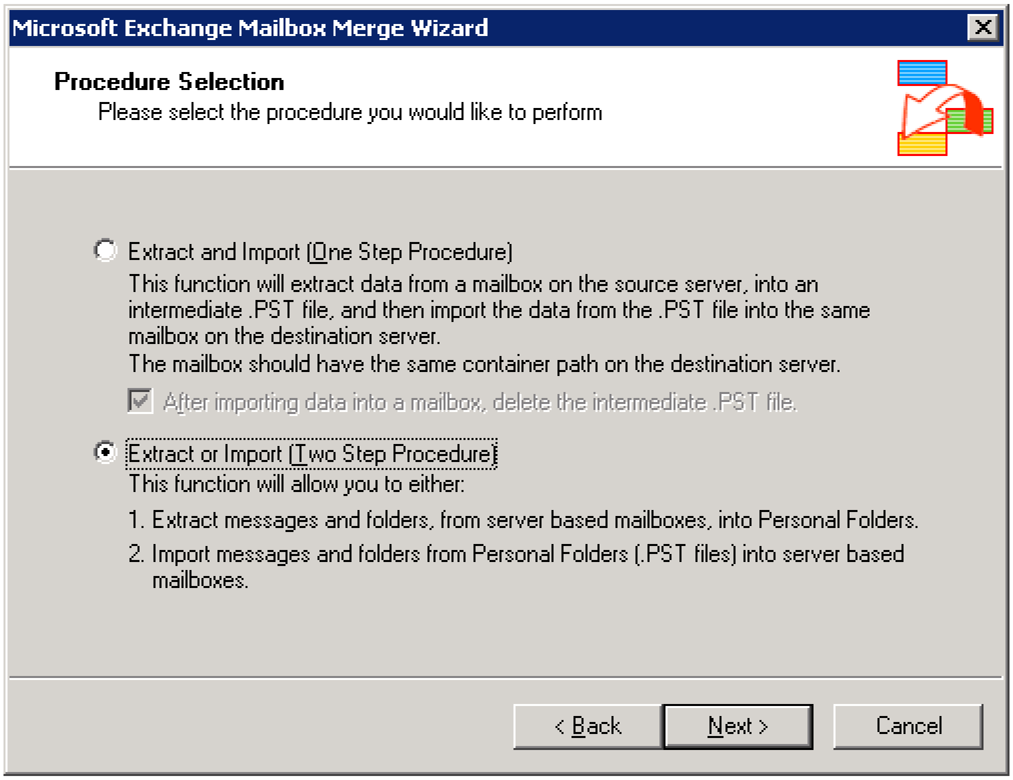
4b. Click **Apply**, and then click **OK**.

4c. Right-click on the database **priv1**, and click **Mount Store**; click **Yes** in the Warning dialog box.

Step 5. Microsoft Exchange Server Mailbox Merge Wizard (ExMerge)

Go to the Microsoft download page, and download **ExMerge.exe** to the **C:\Program Files\Exchsrvr\bin** directory on your Exchange 2003 Server. Once downloaded, double-click **ExMerge.exe** to start the Wizard.
Step 5a. Extract Data from the Exchange Server Mailbox

1. Click **Next** on the **Welcome** page. On the **Procedure Selection** page, select **Extract or Import (Two Step Procedure)**, and then click **Next**:



Procedure Selection

Please select the procedure you would like to perform

○ Extract and Import (One Step Procedure)

This function will extract data from a mailbox on the source server, into an intermediate .PST file, and then import the data from the .PST file into the same mailbox on the destination server.

The mailbox should have the same container path on the destination server.

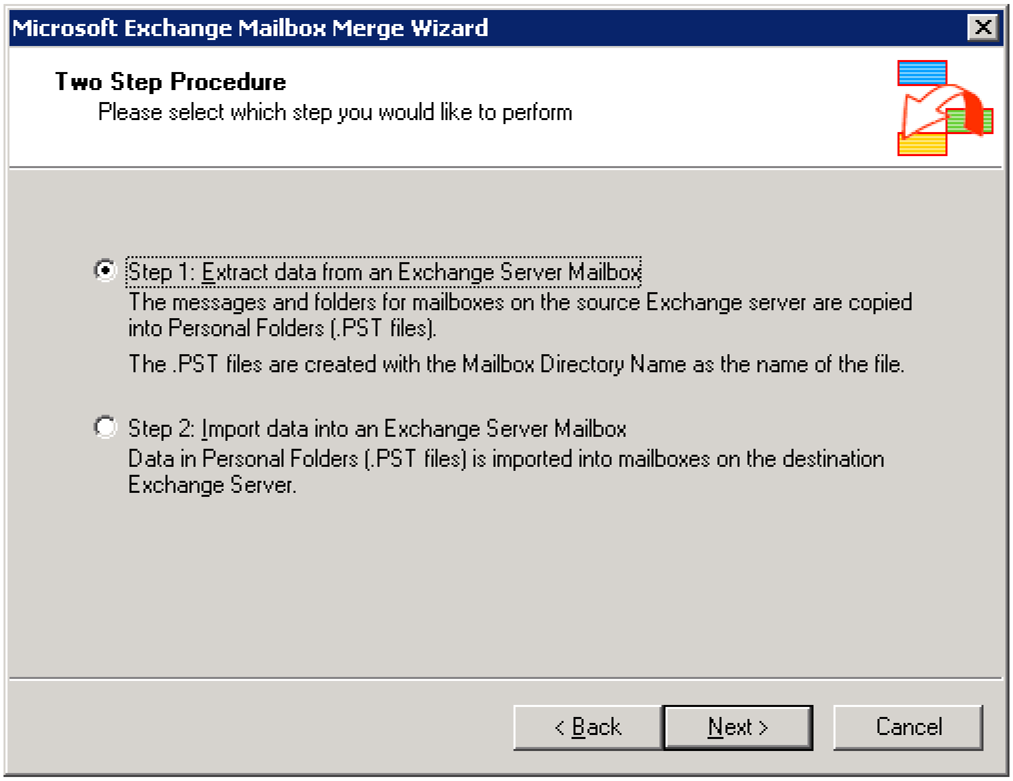
☑ After importing data into a mailbox, delete the intermediate .PST file.

● Extract or Import (Two Step Procedure)

This function will allow you to either:

1. Extract messages and folders, from server based mailboxes, into Personal Folders.
2. Import messages and folders from Personal Folders (.PST files) into server based mailboxes.

2. On the **Two Step Procedure** page, select **Step 1: Extract data from an Exchange Server Mailbox**, and then click **Next**:



Two Step Procedure

Please select which step you would like to perform

● Step 1: Extract data from an Exchange Server Mailbox

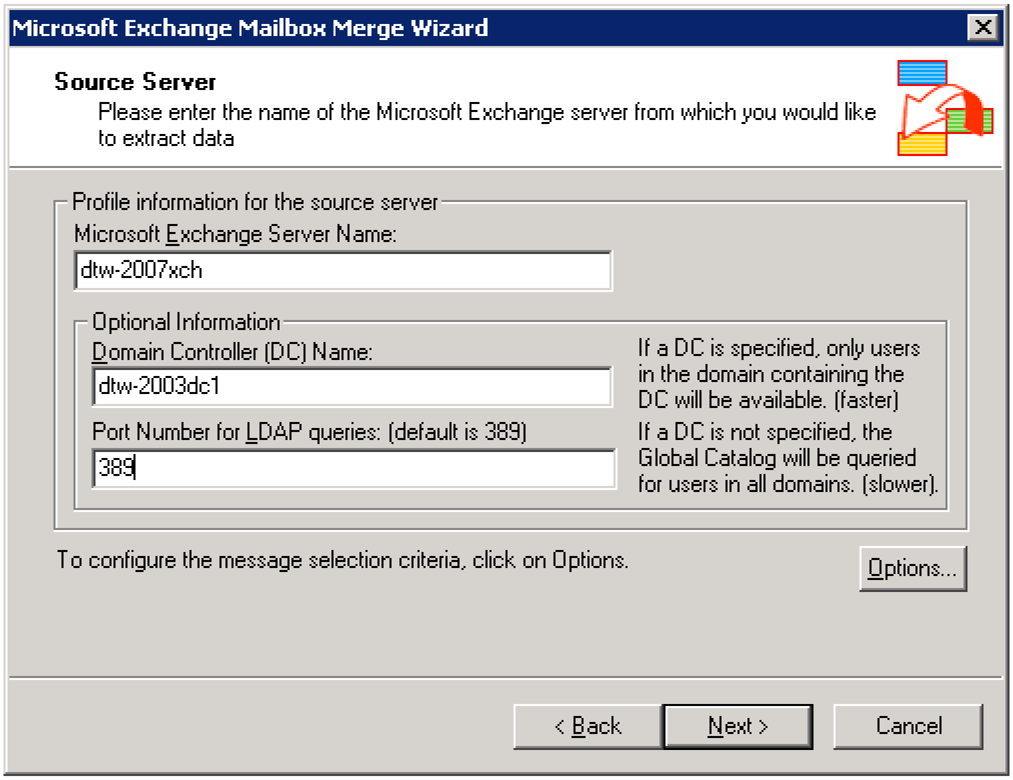
The messages and folders for mailboxes on the source Exchange server are copied into Personal Folders (.PST files).

The .PST files are created with the Mailbox Directory Name as the name of the file.

○ Step 2: Import data into an Exchange Server Mailbox

Data in Personal Folders (.PST files) is imported into mailboxes on the destination Exchange Server.

3. On the **Source Server** page, enter the Exchange Server name, Domain Controller name, and port number in the corresponding fields, and click **Next**:


Microsoft Exchange Mailbox Merge Wizard

Source Server

Please enter the name of the Microsoft Exchange server from which you would like to extract data

Profile information for the source server

Microsoft Exchange Server Name: dtw-2007xch

Optional Information

Domain Controller (DC) Name: dtw-2003dc1

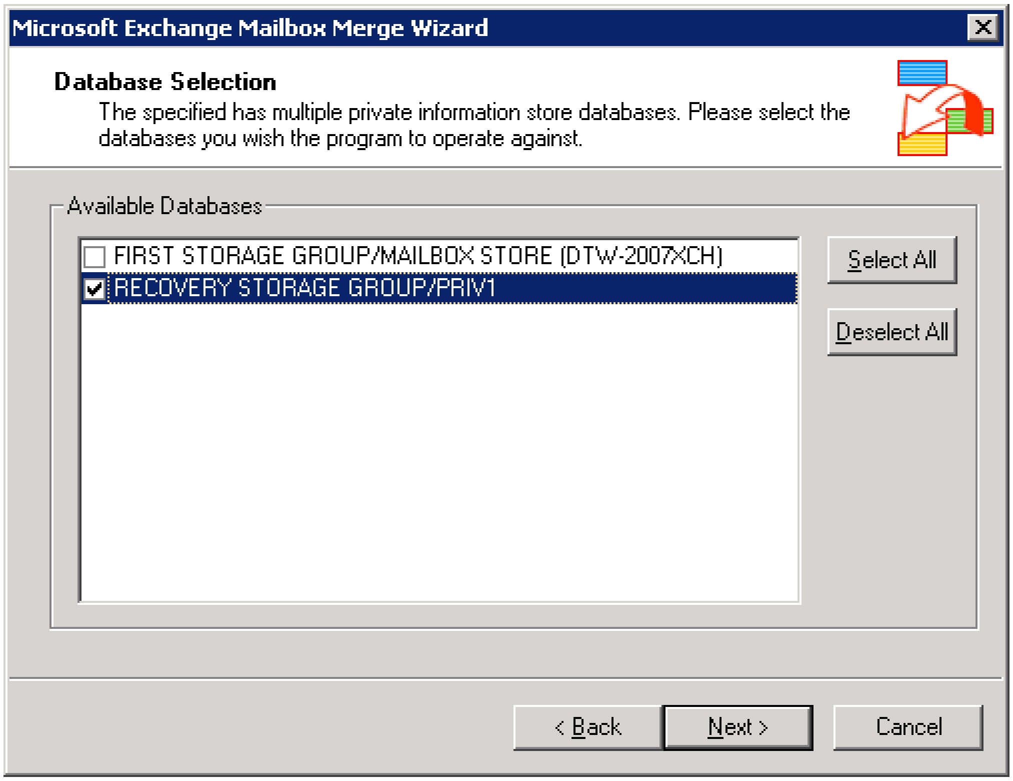
Port Number for LDAP queries: (default is 389) 389

If a DC is specified, only users in the domain containing the DC will be available. (faster)

If a DC is not specified, the Global Catalog will be queried for users in all domains. (slower).

To configure the message selection criteria, click on Options.

4. On the **Database Select** page, select **RECOVERY STORAGE GROUP/** *PRIV1* where *PRIV1* represents the mailstore name you entered in **Step 2e**, and then click **Next**:


Microsoft Exchange Mailbox Merge Wizard

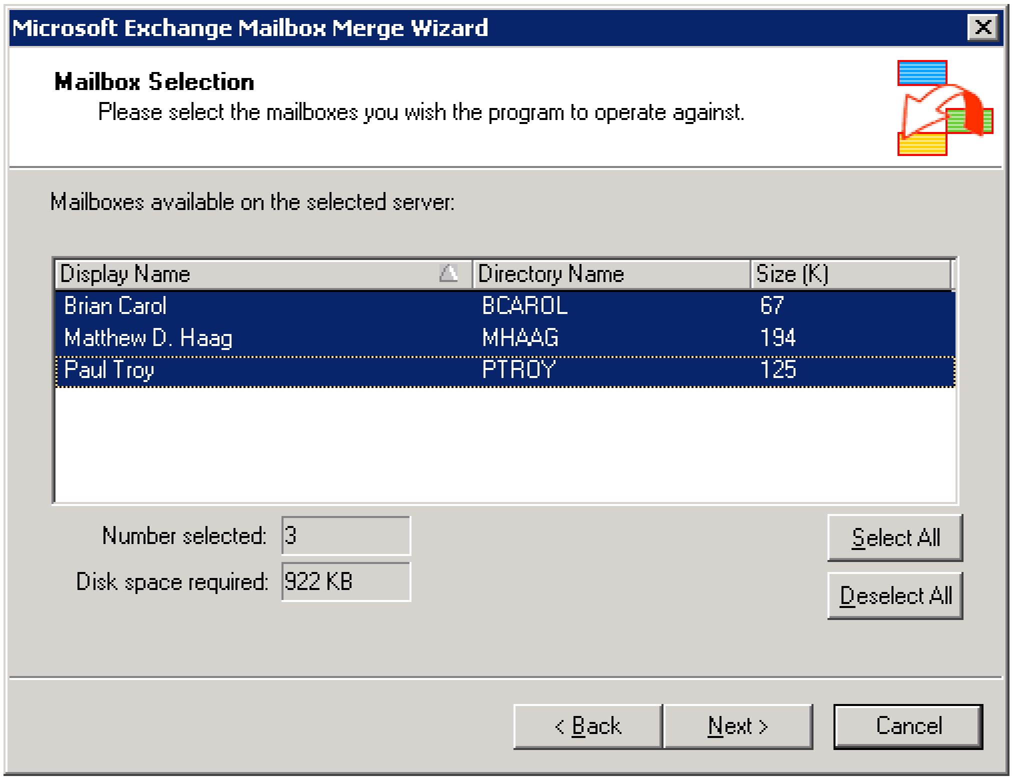
Database Selection

The specified has multiple private information store databases. Please select the databases you wish the program to operate against.

Available Databases

☐ FIRST STORAGE GROUP/MAILBOX STORE (DTW-2007XCH)
☑ RECOVERY STORAGE GROUP/PRIV1

5. On the **Mailbox Selection** page, select all of the mailboxes using **Ctrl-**click, and click **Next**:


Microsoft Exchange Mailbox Merge Wizard

Mailbox Selection

Please select the mailboxes you wish the program to operate against.

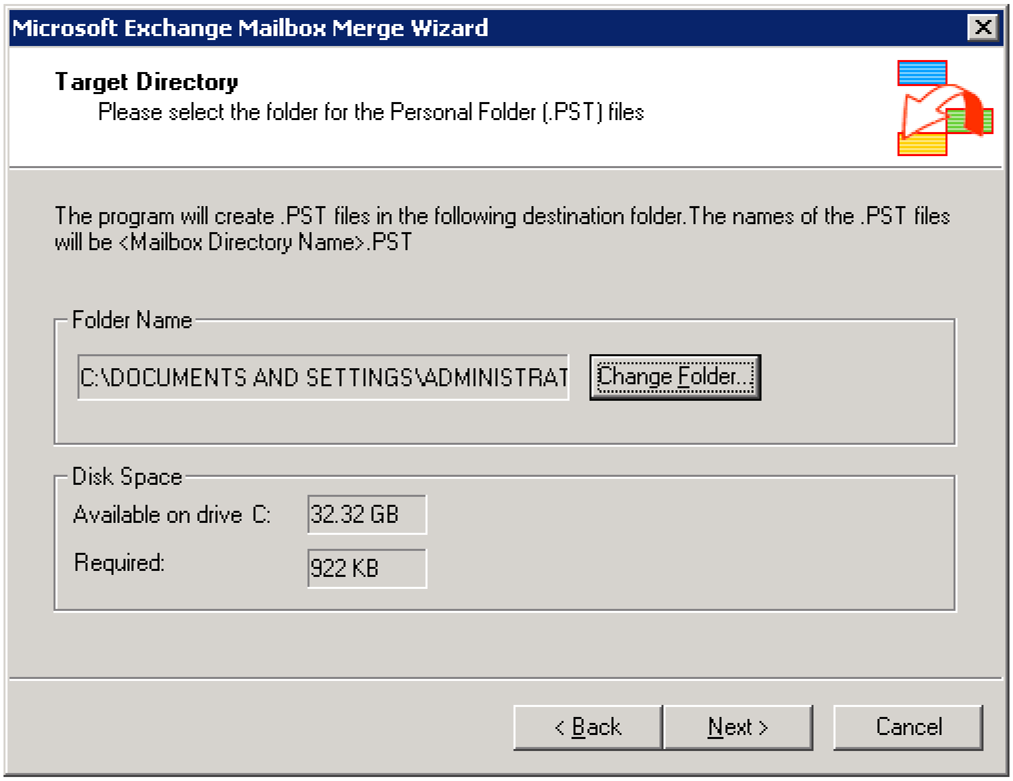
Mailboxes available on the selected server:

Display Name	Directory Name	Size (K)
Brian Carol	BCAROL	67
Matthew D. Haag	MHAAG	194
Paul Troy	PTROY	125

Number selected: 3

Disk space required: 922 KB

6. On the **Locale Selection** page, select the **Default locale**, and then click **Next**.
7. On the **Target Directory** page, click **Change Folder** and choose a target directory for the PST files from which to merge data into the Exchange Server, and then click **Next**:


Microsoft Exchange Mailbox Merge Wizard

Target Directory

Please select the folder for the Personal Folder (.PST) files

The program will create .PST files in the following destination folder. The names of the .PST files will be <Mailbox Directory Name>.PST

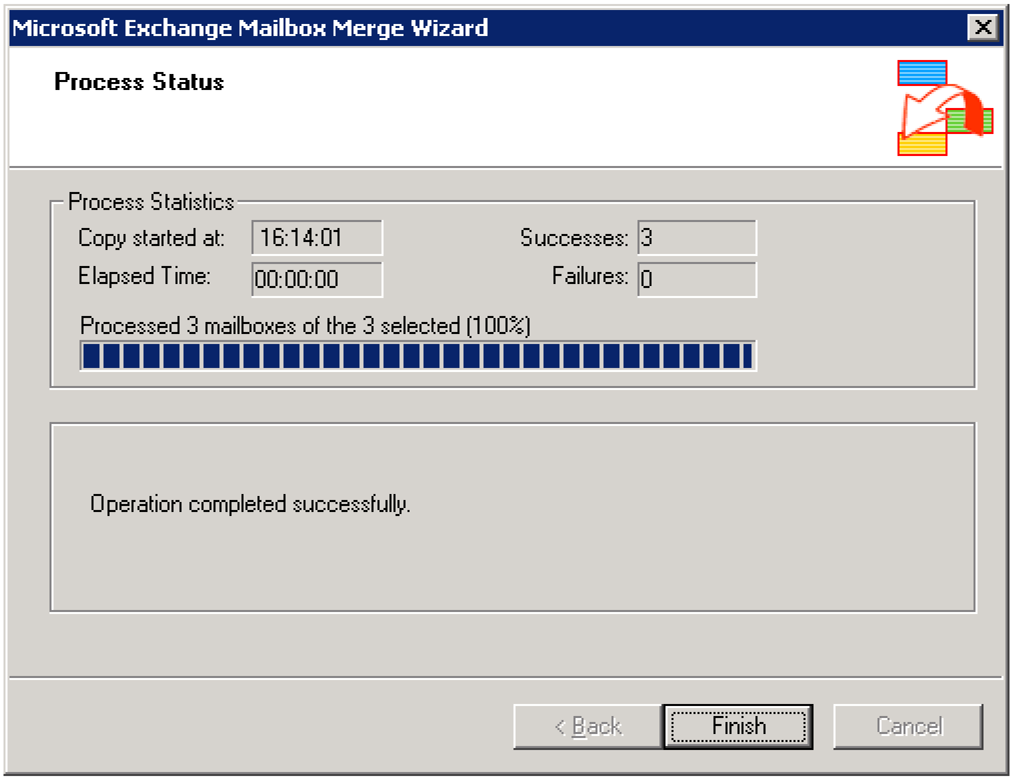
Folder Name: C:\DOCUMENTS AND SETTINGS\ADMINISTRAT

Disk Space

Available on drive C: 32.32 GB

Required: 922 KB

8. On the **Save Settings** page, click **Next**, and on the **Process Status** page, click **Finish**:



Process Status

Process Statistics

Copy started at: 16:14:01

Elapsed Time: 00:00:00

Successes: 3

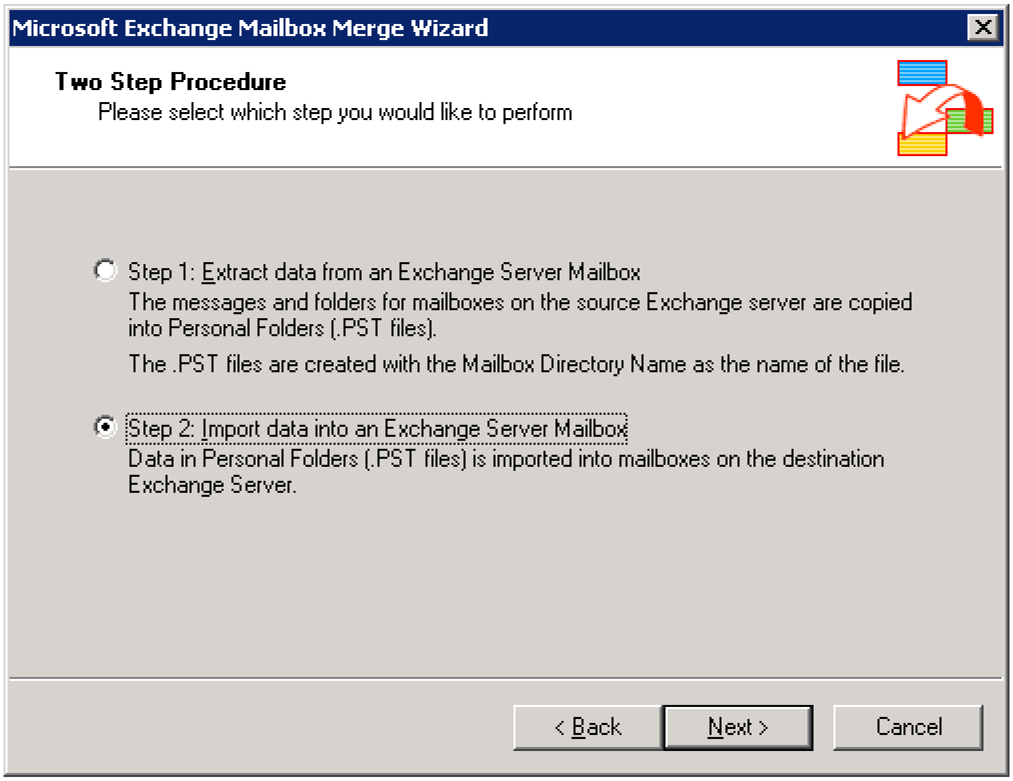
Failures: 0

Processed 3 mailboxes of the 3 selected (100%)

Operation completed successfully.

Step 5b. Import Data into the Exchange Server Mailbox

1. Double-click **ExMerge.exe** to start the Wizard, and click **Next** on the **Welcome** page.
2. On the **Procedure Selection** page, select **Extract or Import (Two Step Procedure)**, and click **Next**.
3. On the **Two Step Procedure** page, select **Step 2: Import data into an Exchange Server Mailbox**, and then click **Next**:



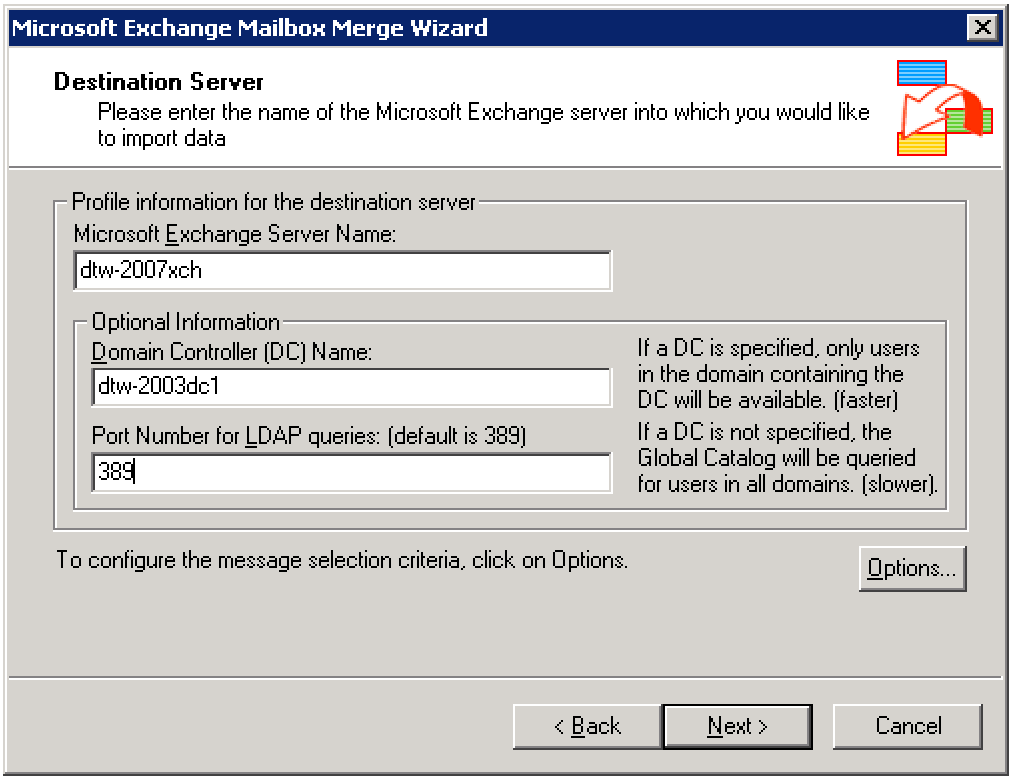
Two Step Procedure

Please select which step you would like to perform

○ Step 1: Extract data from an Exchange Server Mailbox
The messages and folders for mailboxes on the source Exchange server are copied into Personal Folders (.PST files).
The .PST files are created with the Mailbox Directory Name as the name of the file.

● Step 2: Import data into an Exchange Server Mailbox
Data in Personal Folders (.PST files) is imported into mailboxes on the destination Exchange Server.

4. On the **Destination Server** page, enter the server name, Domain Controller name, and port number in the corresponding fields, and click **Next**:



Microsoft Exchange Mailbox Merge Wizard

Destination Server

Please enter the name of the Microsoft Exchange server into which you would like to import data

Profile information for the destination server

Microsoft Exchange Server Name: dtw-2007xch

Optional Information

Domain Controller (DC) Name: dtw-2003dc1

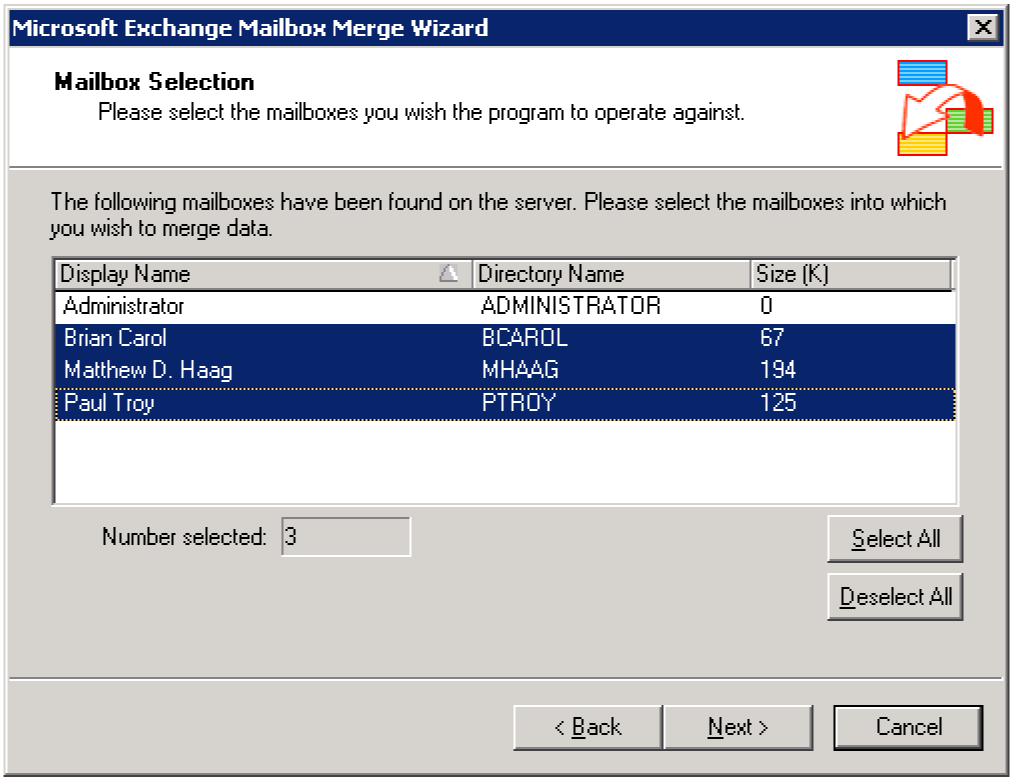
Port Number for LDAP queries: (default is 389) 389

If a DC is specified, only users in the domain containing the DC will be available. (faster)

If a DC is not specified, the Global Catalog will be queried for users in all domains. (slower).

To configure the message selection criteria, click on Options.

5. On the **Mailbox Selection** page, select all of the mailboxes using **Ctrl-**click, and click **Next**:



Microsoft Exchange Mailbox Merge Wizard

Mailbox Selection

Please select the mailboxes you wish the program to operate against.

The following mailboxes have been found on the server. Please select the mailboxes into which you wish to merge data.

Display Name	Directory Name	Size (K)
Administrator	ADMINISTRATOR	0
Brian Carol	BCAROL	67
Matthew D. Haag	MHAAG	194
Paul Troy	PTROY	125

Number selected: 3

6. On the **Locale Selection** page, select the desired locale, and click **Next**. On the **Target Directory** page, click **Change Folder** and select the target folder containing the PST files.
7. On the **Save Settings** page, click **Next**, and on the **Process Status** page, click **Finish**.

Microsoft SQL Server Database Recovery and Restoration

In this Section

- How to Restore a Microsoft SQL Database
- How to Restore a SQL Server 2008 Master Database
- How to Restore a Microsoft SQL Database to a Point-in-Time
- How to Restore a Microsoft SQL Server Database to a Flat File

Related Articles

- How to Change the SQL Recovery Model

How to Restore a Microsoft SQL Database

This article refers to Barracuda Backup firmware version 5.0 or higher.

In this article:

- Restore a SQL User Database
- Restore a SQL Master Database
- Restore a SQL SharePoint Database

Restore a SQL User Database

When you request the restore of a Microsoft SQL Server user database, Barracuda Backup performs all of the restores required to get to the desired date, as follows:

- Restore a full backup of the SQL Server database
- Restore the incremental backups in the order in which they were created

In other words, if you want to restore the database to a certain date, simply select the date and that database, and Barracuda Backup restores all intermediate required database revisions.

ToUse the following steps to restore a Microsoft SQL user database,

1. On the **RESTORE > Restore Browser** page, select the day and time from which you want to restore.
2. Select the data source from which you want to restore.
3. Select the database(s) to restore, and click **Restore**.

Restore a SQL Master Database

If the master database becomes unusable, it must be restored from a previous SQL Dump or backup. All changes made to the master database after the last backup or dump are lost when the dump is reloaded, and therefore must be reapplied.

> A damaged master database is evident by the failure of the SQL Server to start, by segmentation faults, or by input/output errors. The procedure used to recover a damaged master database is different from the procedure used to recover user databases. If the master database becomes unusable, it must be restored from a previous SQL Dump or back up. All changes made to the master database after the last backup or dump are lost when the dump is reloaded and therefore must be reapplied. It is strongly recommended that the master database be backed up each time it is changed.

Use the following steps to recover a damaged master database,

1. Verify that the Barracuda Backup Agent is installed on the local machine.
2. Stop the SQL Server Services using the SQL Server Enterprise Manager.
3. Rebuild the master database; refer to Microsoft Developer Network (MSDN) for detailed procedures for your version of SQL.
4. Initiate Single User Restore Mode on the SQL database by entering the following from a command prompt; leave the window open after executing the command:
   ```
   CD \program files\microsoft sql server\<sql version>\mssql\binn
   sqlservr -c -m (SQL 7)
   sqlservr -c -m -s %<Named Instance>% (SQL 8)
   ```
5. After you complete the restore, remove the `-m` before you restart the server instance in the normal multi-user mode:
   ```
   CD \program files\microsoft sql server\<sql version>\mssql\binn
   sqlservr (SQL 7)
   ```

`sqlservr -s %<Named Instance>% (SQL 8)`

6. If login IDs or devices have been added to or dropped from the master database since the last backup, those changes must be reapplied. Restart the server and reapply the changes manually or from saved batch files.
7. If any databases have been created, expanded, or shrunk since the last dump of the master, those databases must be dropped and then restored. Refer to http://msdn.microsoft.com for detailed procedures for your version of SQL.
8. Close the command prompt.
9. Restart the SQL Service using SQL Enterprise Manager.

Restore a SQL SharePoint Database

Use the following steps to restore a SQL SharePoint database:

1. Start the Windows SharePoint Services VSS Writer service.
2. Start the Volume Shadow Copy service.
3. Shut down any web applications whose content is being restored.

How to Restore a SQL Server 2008 Master Database

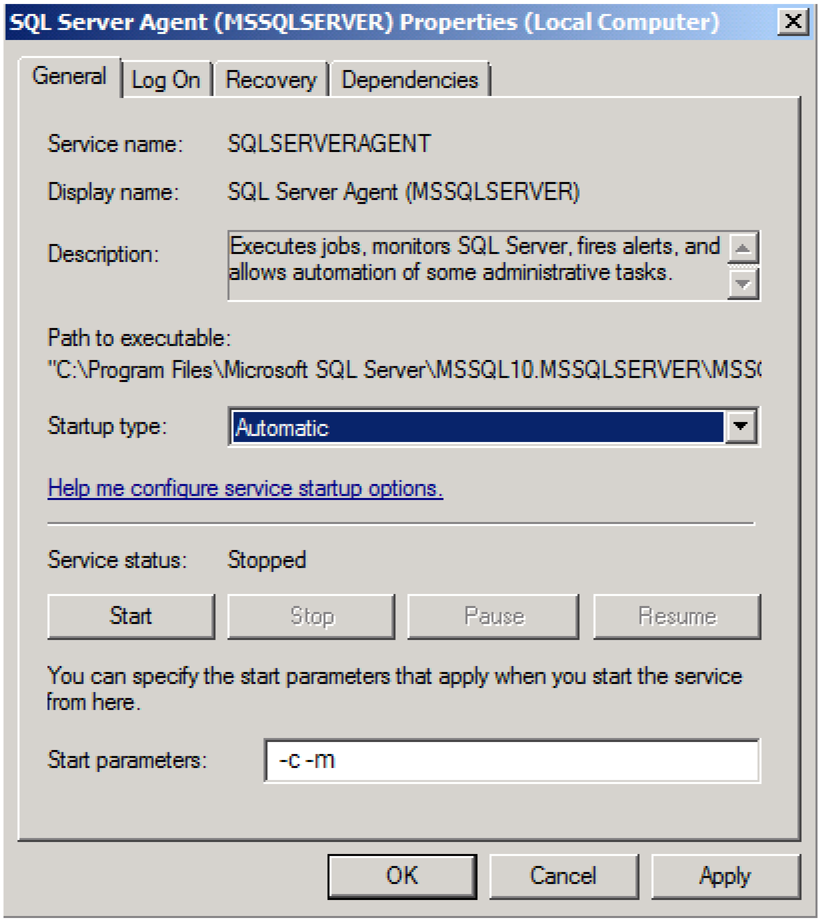
This article refers to all Barracuda Backup firmware versions, and Microsoft ® SQL Server 2005 and 2008.

In this article:

- Set Microsoft SQL Server to Single User Mode
- Stop Services
- Restore the Database
- Set Microsoft SQL Server to Multi-User Mode

Set Microsoft SQL Server to Single User Mode

1. Log in to the SQL server as the administrator.
2. Go to **Administrative Tools > Services**, right-click on the service **SQL Server (MSSQLSERVER)**, and click **Stop**.
3. Double-click **SQL Server (MSSQLSERVER)** to open the **Service Properties** dialog box.
4. Click the **General** tab, and in the **Start parameters** field, type: `-c -m`


SQL Server Agent (MSSQLSERVER) Properties (Local Computer)
General
Log On
Recovery
Dependencies
Help me configure service startup options.
Start
Stop
Pause
Resume
OK
Cancel
Apply

Service name: SQLSERVERAGENT

Display name: SQL Server Agent (MSSQLSERVER)

Description: Executes jobs, monitors SQL Server, fires alerts, and allows automation of some administrative tasks.

Path to executable:
"C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSS

Startup type: Automatic

Service status: Stopped

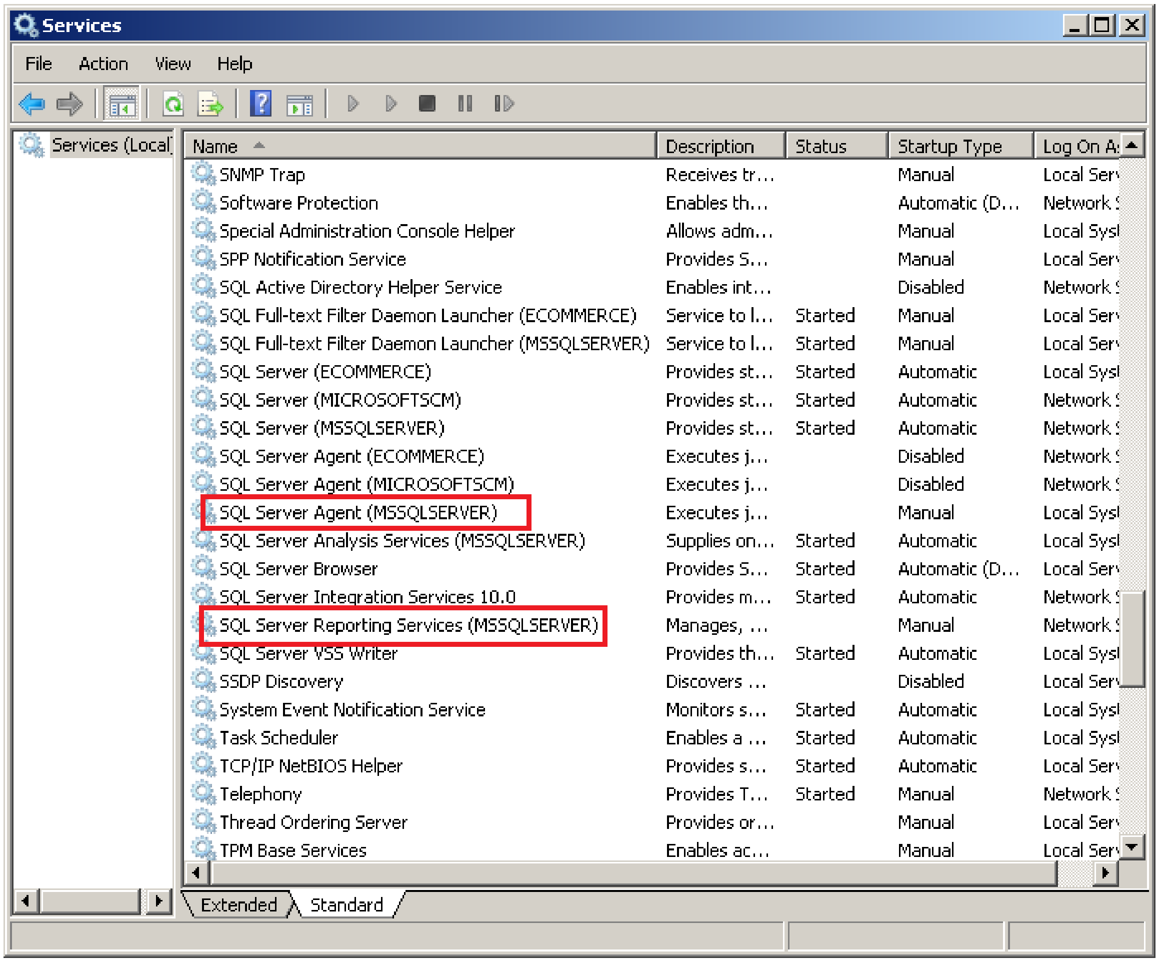
You can specify the start parameters that apply when you start the service from here.

Start parameters: -c -m

5. Click **Start** in the **General** tab to place the server in single user mode, and then click **OK** to close the dialog box.

Stop Services

1. In the **Services** window, right-click on the service **SQL Server Agent (MSSQLSERVER)**, and click **Stop**.
2. In the **Services** window, right-click on the service **SQL Server Reporting (MSSQLSERVER)** service, and click **Stop**:



Name	Description	Status	Startup Type	Log On A
SNMP Trap	Receives tr...		Manual	Local Ser
Software Protection	Enables th...		Automatic (D...	Network
Special Administration Console Helper	Allows adm...		Manual	Local Sys
SPP Notification Service	Provides S...		Manual	Local Ser
SQL Active Directory Helper Service	Enables int...		Disabled	Network
SQL Full-text Filter Daemon Launcher (ECOMMERCE)	Service to l...	Started	Manual	Local Ser
SQL Full-text Filter Daemon Launcher (MSSQLSERVER)	Service to l...	Started	Manual	Local Ser
SQL Server (ECOMMERCE)	Provides st...	Started	Automatic	Local Sys
SQL Server (MICROSOFTSCM)	Provides st...	Started	Automatic	Network
SQL Server (MSSQLSERVER)	Provides st...	Started	Automatic	Network
SQL Server Agent (ECOMMERCE)	Executes j...		Disabled	Network
SQL Server Agent (MICROSOFTSCM)	Executes j...		Disabled	Network
SQL Server Agent (MSSQLSERVER)	Executes j...		Manual	Local Sys
SQL Server Analysis Services (MSSQLSERVER)	Supplies on...	Started	Automatic	Local Sys
SQL Server Browser	Provides S...	Started	Automatic (D...	Local Ser
SQL Server Integration Services 10.0	Provides m...	Started	Automatic	Network
SQL Server Reporting Services (MSSQLSERVER)	Manages, ...		Manual	Network
SQL Server VSS Writer	Provides th...	Started	Automatic	Local Sys
SSDP Discovery	Discovers ...		Disabled	Local Ser
System Event Notification Service	Monitors s...	Started	Automatic	Local Sys
Task Scheduler	Enables a ...	Started	Automatic	Local Sys
TCP/IP NetBIOS Helper	Provides s...	Started	Automatic	Local Ser
Telephony	Provides T...	Started	Manual	Network
Thread Ordering Server	Provides or...		Manual	Local Ser
TPM Base Services	Enables ac...		Manual	Local Ser

Restore the Database

1. Log in to Barracuda Backup, go to the **Restore > Restore Browser** page.
2. Click **Restore** next to the Microsoft SQL Server instance to restore.
3. In the **Restore** dialog box, select to restore to the original instance or a new instance, and click **Start Restore**.

Set Microsoft SQL Server to Multi-User Mode

1. Log in to the SQL server as the administrator.
2. Go to **Administrative Tools > Services**, right-click on the following services, and click **Start**:
    - **SQL Server (MSSQLSERVER)**
    - **SQL Server Agent (MSSQLSERVER)**
    - **SQL Server Reporting Services (MSSQLSERVER)**

How to Restore a Microsoft SQL Database to a Point-in-Time

> This article refers to all Barracuda Backup firmware releases, and Microsoft SQL Server 2000, 2005, and 2008, using Microsoft SQL Server Management Studio.

In this article:

- Restoring the Database
- Restoring to a Point-in-Time

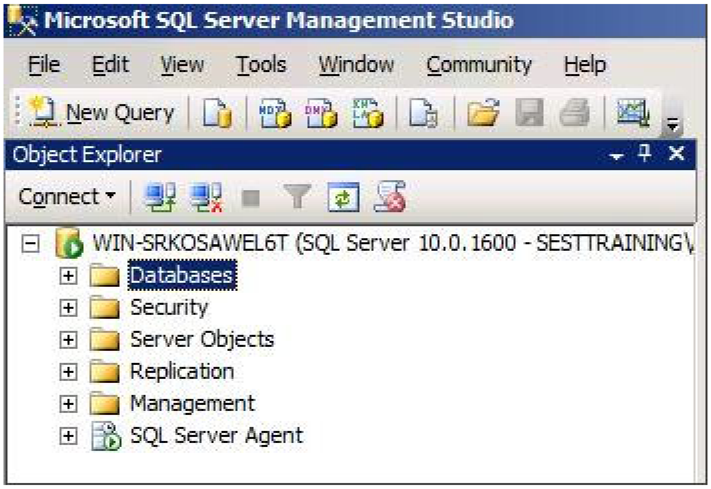
Related Articles
- Restore to a Flat File

Flat File
This article describes how to restore a SQL database to a point-in-time, and then restore the database to working condition using SQL Management Studio. Before completing this solution, you must first Restore the Microsoft Database to a Flat File.

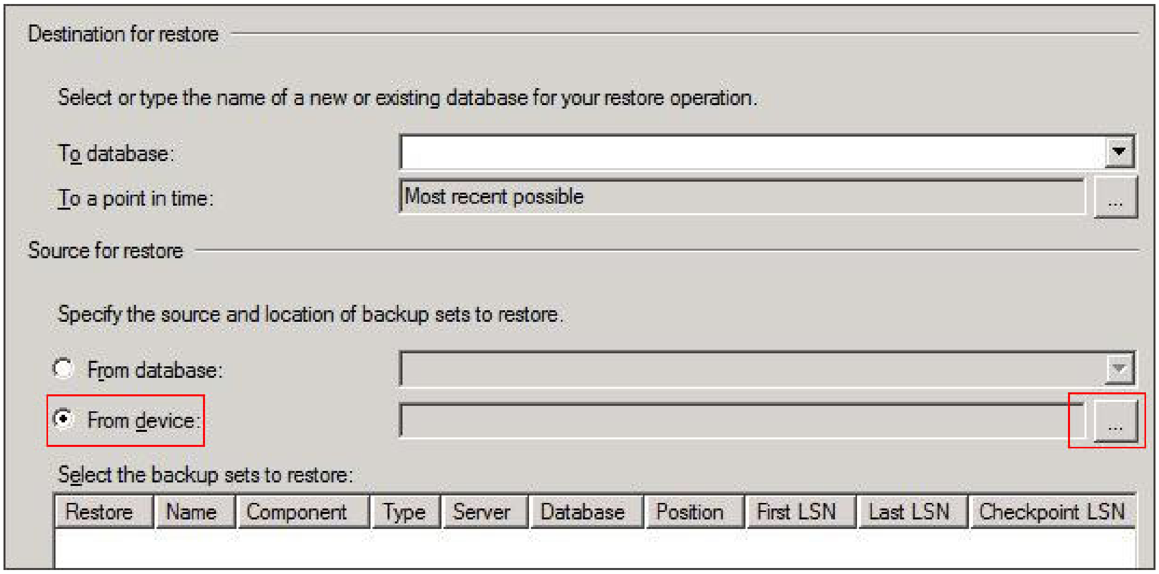
Restoring the Database

Use the following steps to restore the database:

1. Open Microsoft SQL Server Management Studio, and navigate to **Databases**:


Microsoft SQL Server Management Studio
File
Edit
View
Tools
Window
Community
Help
New Query
Object Explorer
Connect
WIN-SRKOSAWEL6T (SQL Server 10.0.1600 - SESTTRAINING\
Databases
Security
Server Objects
Replication
Management
SQL Server Agent

2. Right-click **Databases**, and click **Restore Database**. In the **Source for restore** section, select **From Device**, and click the browse button:


Destination for restore

Select or type the name of a new or existing database for your restore operation.

To database:

To a point in time: Most recent possible

Source for restore

Specify the source and location of backup sets to restore.

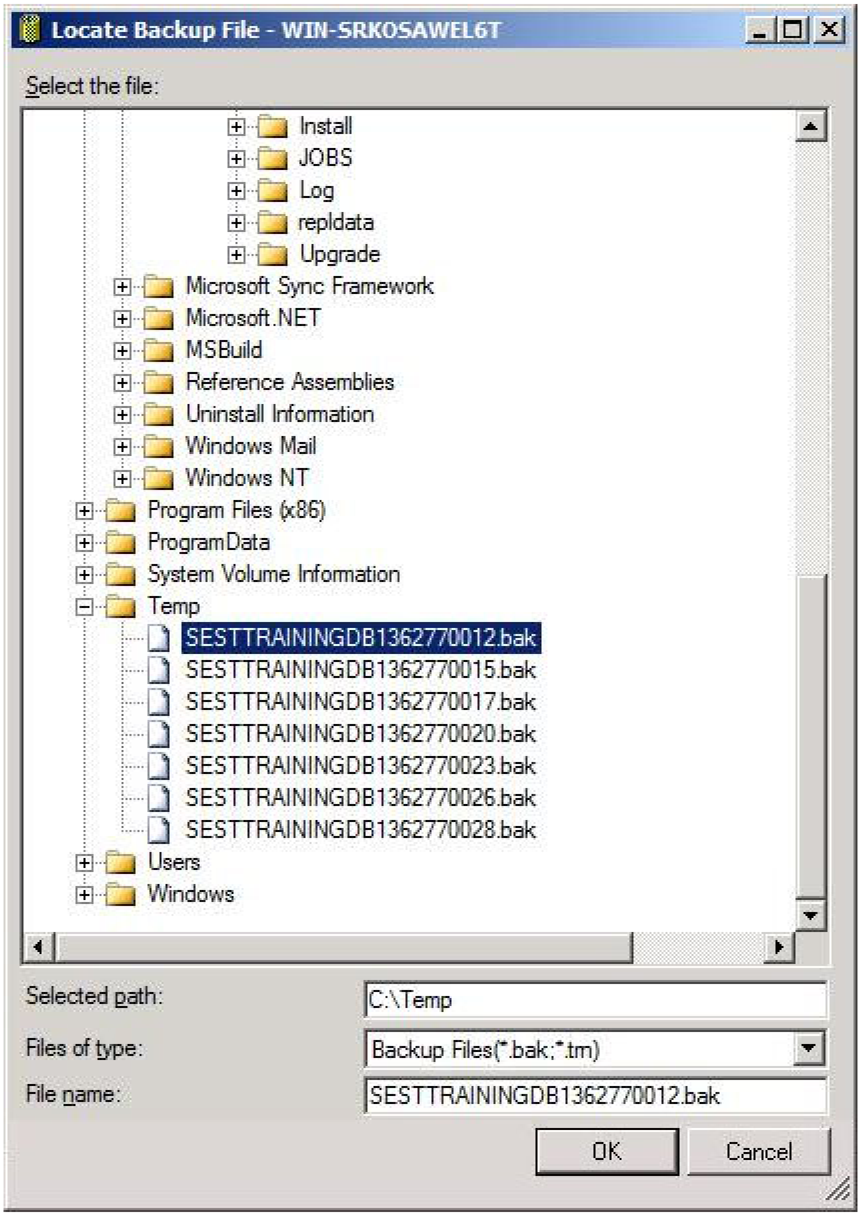
○ From database:

● From device:

Select the backup sets to restore:

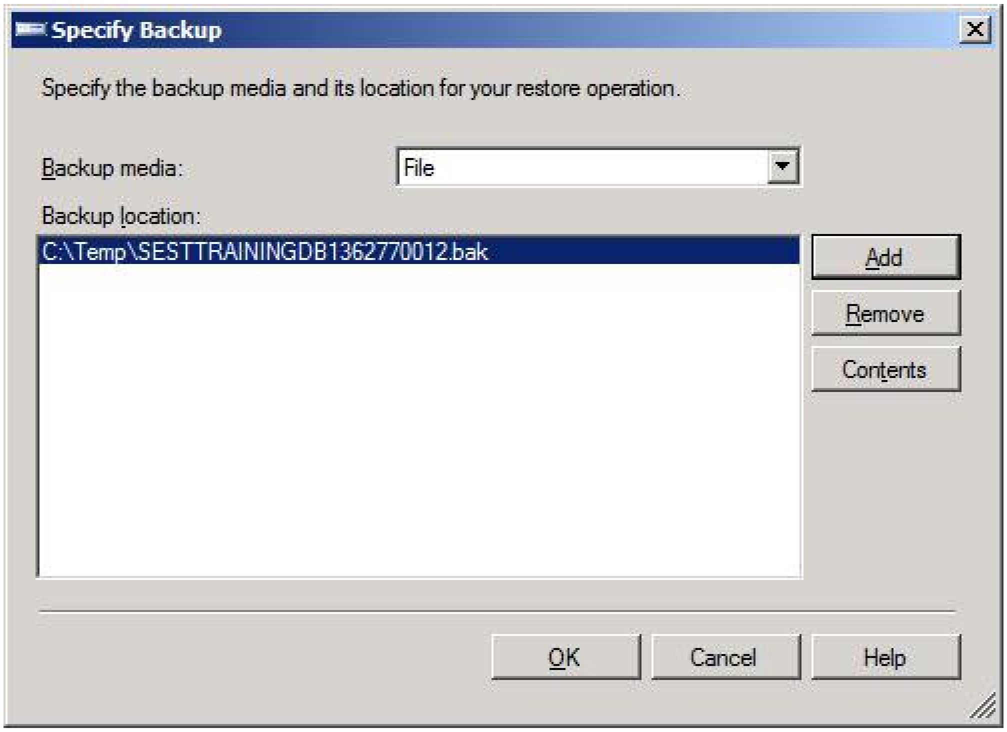
Restore	Name	Component	Type	Server	Database	Position	First LSN	Last LSN	Checkpoint LSN

3. Click **Add** in the **Specify Backup** window. Browse to the location of your recently restored flat files. Choose the Full backup file which should be the first backup file in the list:


Locate Backup File - WIN-SRKOSAWEL6T
Select the file:
Install
JOBS
Log
repldata
Upgrade
Microsoft Sync Framework
Microsoft.NET
MSBuild
Reference Assemblies
Uninstall Information
Windows Mail
Windows NT
Program Files (x86)
ProgramData
System Volume Information
Temp
SESTTRAININGDB1362770012.bak
SESTTRAININGDB1362770015.bak
SESTTRAININGDB1362770017.bak
SESTTRAININGDB1362770020.bak
SESTTRAININGDB1362770023.bak
SESTTRAININGDB1362770026.bak
SESTTRAININGDB1362770028.bak
Users
Windows
OK
Cancel

Selected path: C:\Temp
Files of type: Backup Files(*.bak;*.trn)
File name: SESTTRAININGDB1362770012.bak

4. Click **OK**; the **Specify Backup** window displays:



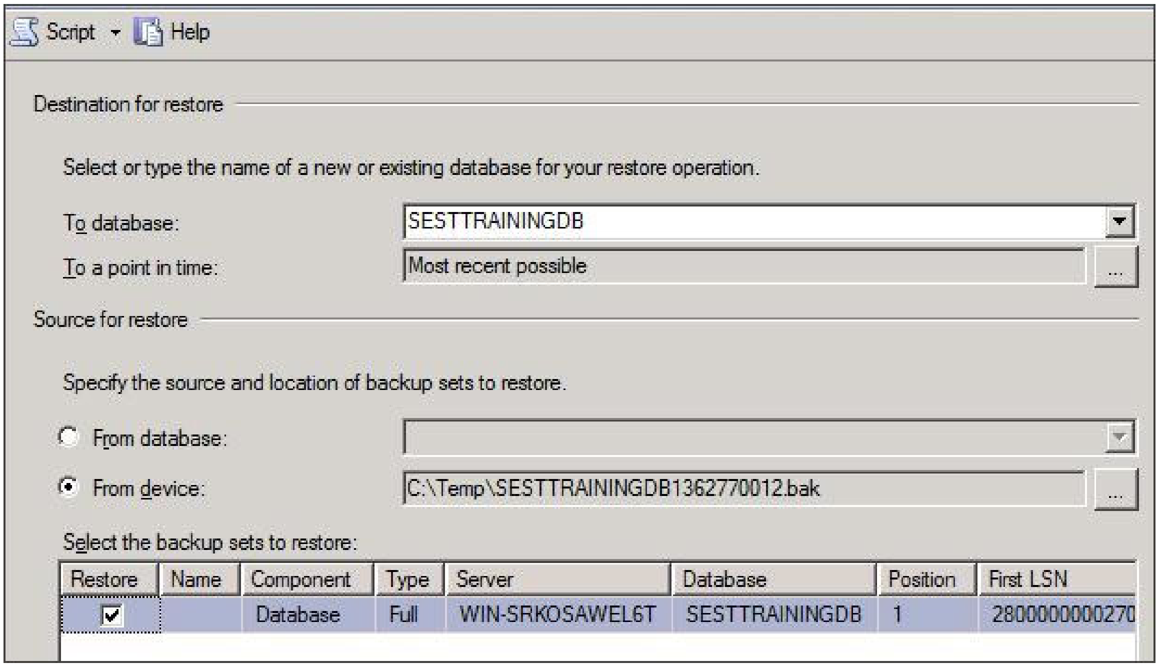
Specify the backup media and its location for your restore operation.

Backup media: File

Backup location:

C:\Temp\SESTTRAININGDB1362770012.bak

5. Click **OK**. In the **Destination for restore** section, select the database to which you wish to restore, and in the **Select the backup sets to restore** section, select the backup file you selected above in step **3**:



Select or type the name of a new or existing database for your restore operation.

To database: SESTTRAININGDB

To a point in time: Most recent possible

Specify the source and location of backup sets to restore.

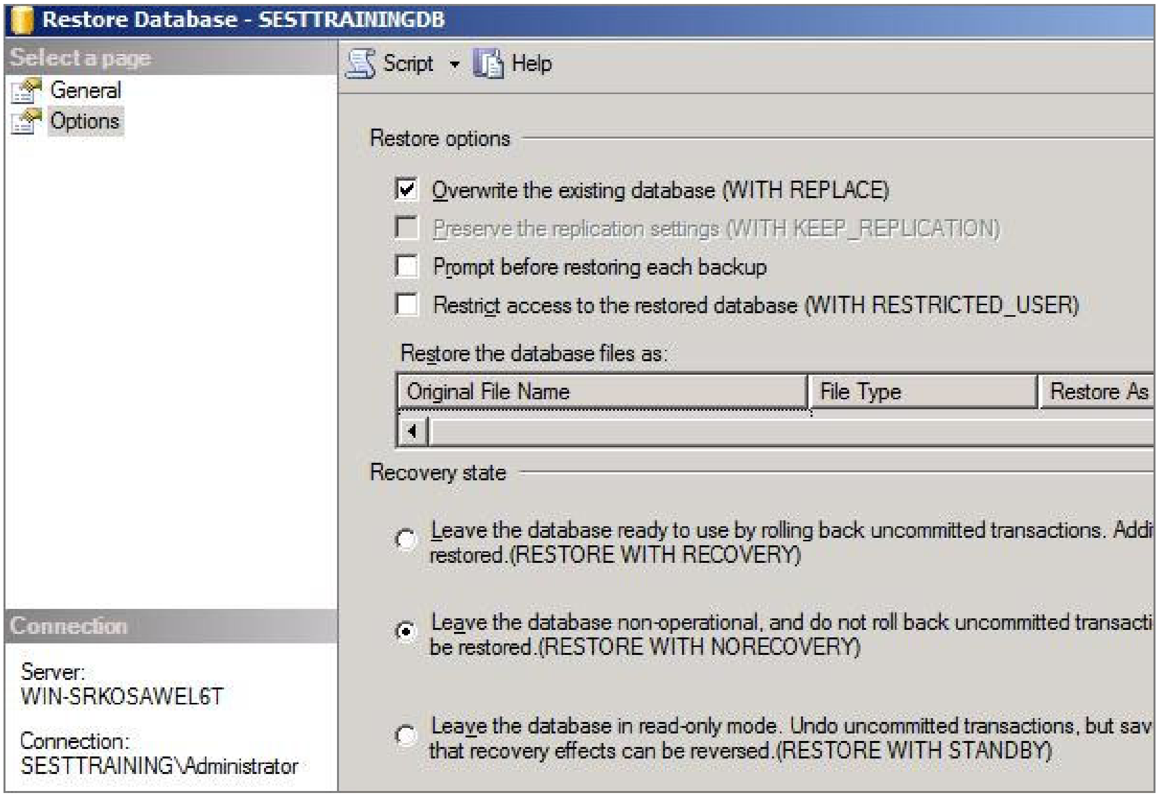
○ From database:

● From device: C:\Temp\SESTTRAININGDB1362770012.bak

Select the backup sets to restore:

Restore	Name	Component	Type	Server	Database	Position	First LSN
☑		Database	Full	WIN-SRKOSAWEL6T	SESTTRAININGDB	1	2800000000270

6. In the left pane, click **Options**, and select the following:
   - In the **Restore options** section, select **Overwrite the existing database (WITH REPLACE)**, and leave the other options unselected.
   - In the **Recovery state** section, select **Leave the database non-operational, and do not roll back uncommited transactions. Additional transaction logs can be restored. (RESTORE WITH NORECOVERY)**:



Restore options

☑ Overwrite the existing database (WITH REPLACE)

☐ Preserve the replication settings (WITH KEEP_REPLICATION)

☐ Prompt before restoring each backup

☐ Restrict access to the restored database (WITH RESTRICTED_USER)

Restore the database files as:

Original File Name	File Type	Restore As

Recovery state

○ Leave the database ready to use by rolling back uncommitted transactions. Addi restored.(RESTORE WITH RECOVERY)

● Leave the database non-operational, and do not roll back uncommitted transacti be restored.(RESTORE WITH NORECOVERY)

○ Leave the database in read-only mode. Undo uncommitted transactions, but sav that recovery effects can be reversed.(RESTORE WITH STANDBY)

Server:
WIN-SRKOSAWEL6T

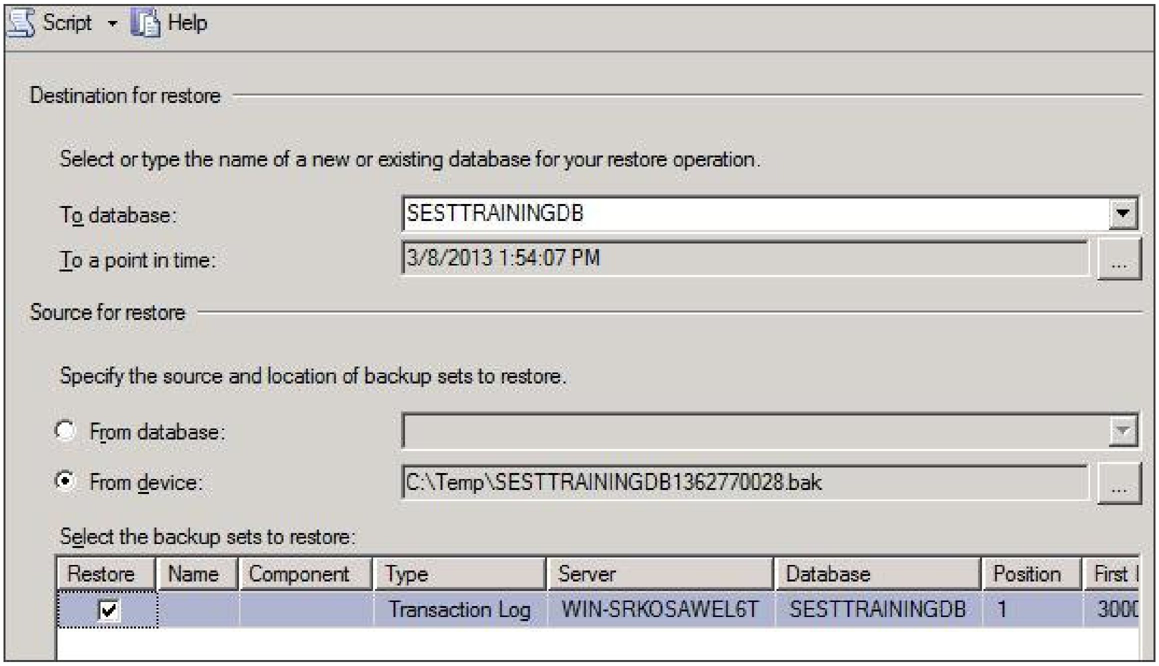
Connection:
SESTTRAINING\Administrator

7. Click **OK** to perform the restore.
8. If the restore is successful, complete steps 1 through 7 for each incremental backup file, which includes the **.tm** file extension, until you reach the incremental file containing the point-in-time file to which you wish to restore.

Restoring to a Point-in-Time

Use the following steps to restore the last incremental file containing the point-in-time:

1. In Microsoft SQL Server Management Studio, right-click **Databases**, and click **Restore Database**.
2. In the **Source for restore** section, select **From Device**, and click the browse button.
3. Click **Add** in the **Specify Backup** window. Browse to the location of your recently restored flat files, select the incremental backup file containing the point-in-time to restore to, and click **OK**.
4. Click **OK** in the **Specify Backup** window. In the **Select the backup sets to restore section**, check the backup file you added in step **3**.
5. In the **Destination for restore** section, select the database to which to restore:



Destination for restore

Select or type the name of a new or existing database for your restore operation.

To database: SESTTRAININGDB

To a point in time: 3/8/2013 1:54:07 PM

Source for restore

Specify the source and location of backup sets to restore.

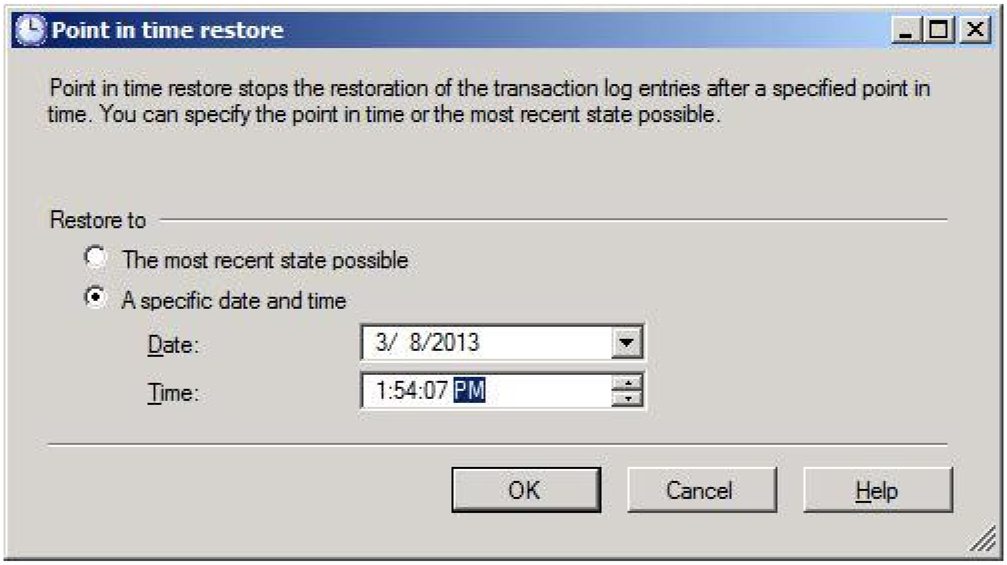
○ From database:

● From device: C:\Temp\SESTTRAININGDB1362770028.bak

Select the backup sets to restore:

Restore	Name	Component	Type	Server	Database	Position	First
☑			Transaction Log	WIN-SRKOSAWEL6T	SESTTRAININGDB	1	300

6. In the **Destination for restore section**, click the browse button following **To a point in time**; the **Point in time restore** window displays.
7. Select **a specific date and time**, and choose the date and time to which to restore:



Point in time restore stops the restoration of the transaction log entries after a specified point in time. You can specify the point in time or the most recent state possible.

Restore to

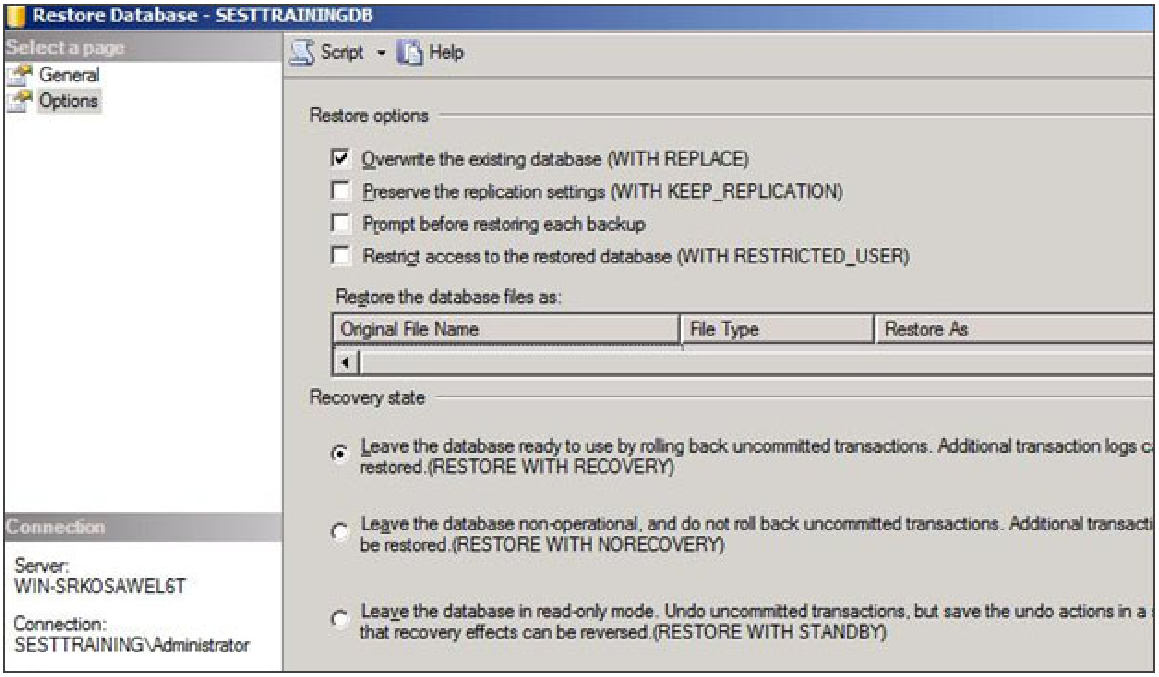
○ The most recent state possible

● A specific date and time

Date: 3/ 8/2013

Time: 1:54:07 PM

8. Click **OK**. In the left pane, click **Options**, and make the following selections:
   - In the **Restore options** section, select **Overwrite the existing database**, and leave the other options unselected.
   - In the **Recovery state** section, select **Leave the database ready to use by rolling back uncommitted transactions. Additional transaction logs can be restored. (RESTORE WITH RECOVERY)**:



Restore options

☑ Overwrite the existing database (WITH REPLACE)
☐ Preserve the replication settings (WITH KEEP_REPLICATION)
☐ Prompt before restoring each backup
☐ Restrict access to the restored database (WITH RESTRICTED_USER)

Restore the database files as:

Original File Name	File Type	Restore As

Recovery state

● Leave the database ready to use by rolling back uncommitted transactions. Additional transaction logs c restored.(RESTORE WITH RECOVERY)
○ Leave the database non-operational, and do not roll back uncommitted transactions. Additional transacti be restored.(RESTORE WITH NORECOVERY)
○ Leave the database in read-only mode. Undo uncommitted transactions, but save the undo actions in a that recovery effects can be reversed.(RESTORE WITH STANDBY)

Server:
WIN-SRKOSAWEL6T

Connection:
SESTTRAINING\Administrator

9. Click **OK** to perform the restore. the restored database should display with only the changes up to the specified point-in-time.

How to Restore a Microsoft SQL Server Database to a Flat File

This article refers to Barracuda Backup firmware 5.1 and lower, and Microsoft SQL Server 2005 and 2008 Windows Agent.

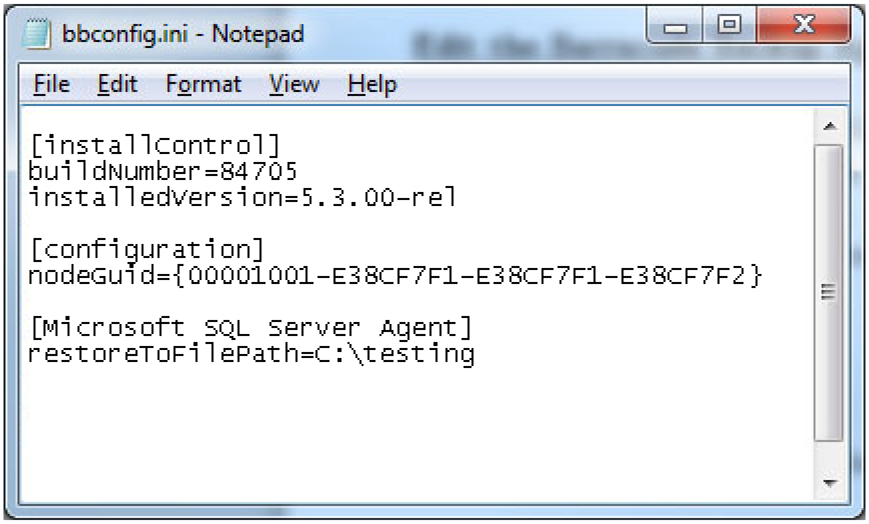
In this article:

- Step 1. Modify the bbconfig.ini File
- Step 2. Restore the Database
- Step 3. Restoring a Flat File into SQL Management Studio

Related Articles
• Restore to a Point-in-Time

Step 1. Modify the bbconfig.ini File

1. On the Microsoft SQL Server where you installed the Barracuda Backup Agent, open Services.
2. Right-click on the Service **Barracuda Backup Agent**, and click **Stop**. The Service is now stopped.
3. Open the **bbconfig.ini** file in Notepad; the file is located in the following directory:
4. ***/Program Files/Barracuda/Barracuda Backup Agent/config/bbconfig.ini***
5. Add the following lines to the end of the file, where *`path to file`* represents the restore path:
   `restoreToFilePath=`*`path to file`*
   For example:



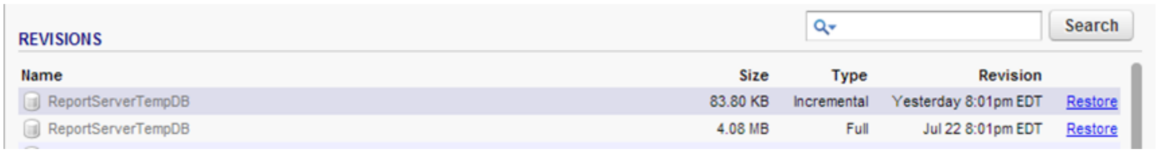
```
[installControl]
buildNumber=84705
installedversion=5.3.00-rel

[configuration]
nodeGuid={00001001-E38CF7F1-E38CF7F1-E38CF7F2}

[Microsoft SQL Server Agent]
restoreToFilePath=C:\testing
```

6. Save and close the file.
7. Open Services once again.
8. Right-click on the Service **Barracuda Backup Agent**, and click **Start**. The **Status** field should display as **Started.**

Step 2. Restore the Database

Use the following steps to restore the database normally through the Barracuda Restore Browser to the path specified in Step 1:

1. Log in to Barracuda Backup, and go to **RESTORE > Restore Browser**.
2. Drill down to and select the database revision to restore, and click **Restore**.
3. In the **Restore** dialog, from the **Restore to** drop-down menu, select the appropriate server.
4. In the **Path** section, select the second option, and enter the path specified in Step 1 in the **bbconfig.ini** file; click **Start Restore**.
5. The database is restored to the server as a **.bak** file if this is a full restore, and to a **.trn** file if this is an incremental backup:



Name	Size	Type	Revision	
ReportServerTempDB	83.80 KB	Incremental	Yesterday 8:01pm EDT	Restore
ReportServerTempDB	4.08 MB	Full	Jul 22 8:01pm EDT	Restore

Step 3. Restoring a Flat File into SQL Management Studio

> **Restoring to a Point-in-Time**
> Once you create the flat file, you can select to restore the Microsoft SQL Database to a Point-in-Time.

Use the following steps to restore the flat file into SQL Management Studio:

1. After connecting to the appropriate instance of the Microsoft SQL Server Database Engine, in Object Explorer, click the **server name** to expand the server tree.
2. Expand **Databases**, and, depending on the database, either select a user database or expand System Databases and select a system database.
3. Right-click the database, point to **Tasks**, and then click **Restore**.
4. Click the type of restore operation you want (**Database**, **Files and Filegroups**, or **Transaction Log**). The corresponding restore dialog box opens.
5. On the **General** page, in the **Restore source** section, click **From device**.
6. Click the **browse** button for the **From device** text box; the **Specify Backup** dialog box displays.
7. From the **Backup media** menu, select **Backup Device**, and click **Add**; the **Select Backup Device** dialog opens.
8. In the **Backup device** menu, select the device you want to use for the restore operation.

Microsoft Hyper-V Recovery and Restoration

In this Section

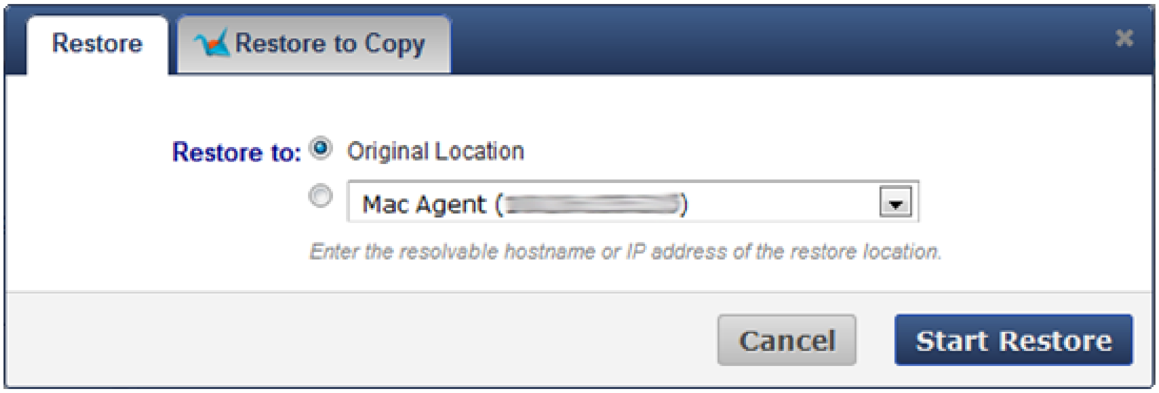
- How to Restore a Microsoft Hyper-V 2012 to its Original Location
- How to Restore a Microsoft Hyper-V Virtual Machine

How to Restore a Microsoft Hyper-V 2012 to its Original Location

> This article refers to Barracuda Backup Server firmware version 5.3 and higher, and Microsoft® Hyper-V 2012 and 2012 R2. This article assumes Hyper-V is installed and configured.

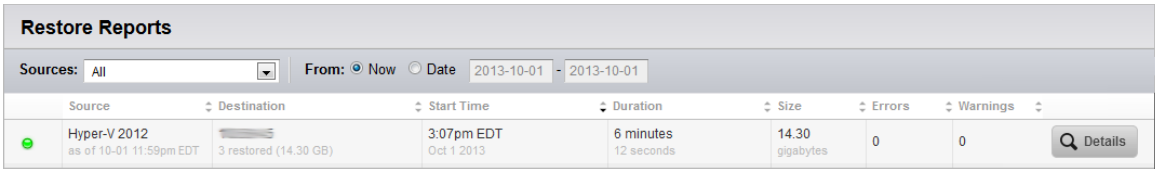
Use the following steps to restore a Hyper-V virtual machine (VM) back to its original location.

1. Turn off or remove the original VM; the restore job will fail if the VM is running.
2. Log in to the Barracuda Backup web interface, select the associated Barracuda Backup Server in the left pane, and go to the **RESTORE > Restore Browser** page.
3. Select the Hyper-V source that contains the VM you want to restore.
4. In the **Contents** list, click **Restore** to the right of the VM.
5. In the **Restore** dialog box, select **Original Location**, and then click **Start Restore**:


Restore
Restore to Copy
Cancel
Start Restore

Restore to: ● Original Location
○ Mac Agent ([redacted])
Enter the resolvable hostname or IP address of the restore location.

6. Go to the **REPORTS > Restore** page to monitor the backup progress:

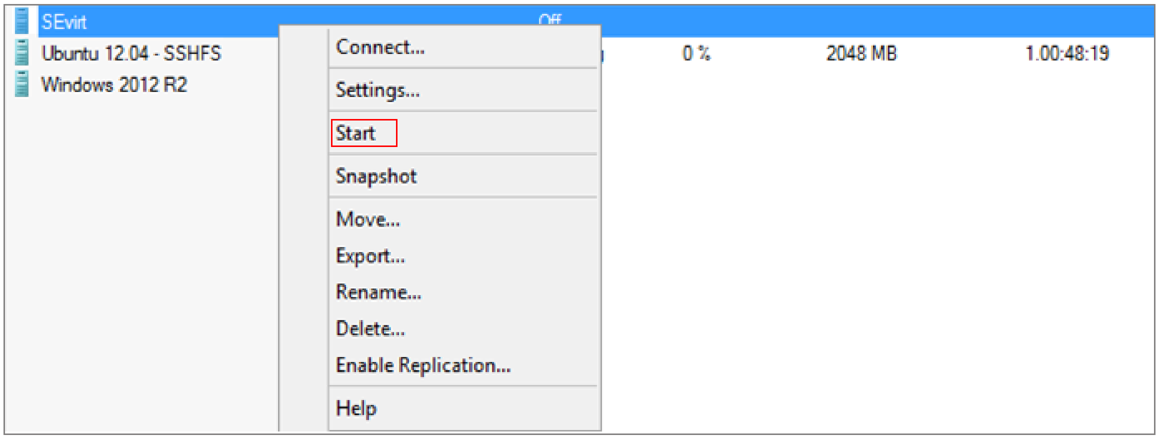


Restore Reports

Sources: All From: ● Now ○ Date 2013-10-01 - 2013-10-01

	Source	Destination	Start Time	Duration	Size	Errors	Warnings	
●	Hyper-V 2012 as of 10-01 11:59pm EDT	[redacted] 3 restored (14.30 GB)	3:07pm EDT Oct 1 2013	6 minutes 12 seconds	14.30 gigabytes	0	0	Details

7. Once the restore is complete, log in to Hyper-V, and then start the server:


SEvirt
Off
Ubuntu 12.04 - SSHFS
0 %
2048 MB
1.00:48:19
Windows 2012 R2
Connect...
Settings...
Start
Snapshot
Move...
Export...
Rename...
Delete...
Enable Replication...
Help

How to Restore a Microsoft Hyper-V Virtual Machine

> This article refers to Barracuda Backup Server firmware version 5.2 and higher, and assumes that Microsoft® Hyper-V is installed and configured.

When restoring a Hyper-V virtual machine back to its original location, keep the following in mind:

- Message-level data must be restored to the computer from which it originally came;
- File share data *cannot* be restored to its original location.

- Restore Data
- Import the Virtual Machine

Related Articles

- How to Set Up Microsoft Hyper-V Virtual Machine Backups

Additional Resources

- Barracuda Networks Knowledgebase Solution #00005702

High Availability
When restoring a high availability (HA) Hyper-V virtual machine, if the virtual machine still exists *anywhere* in the cluster, to avoid restore errors, you must first complete one of the following options before restoring:

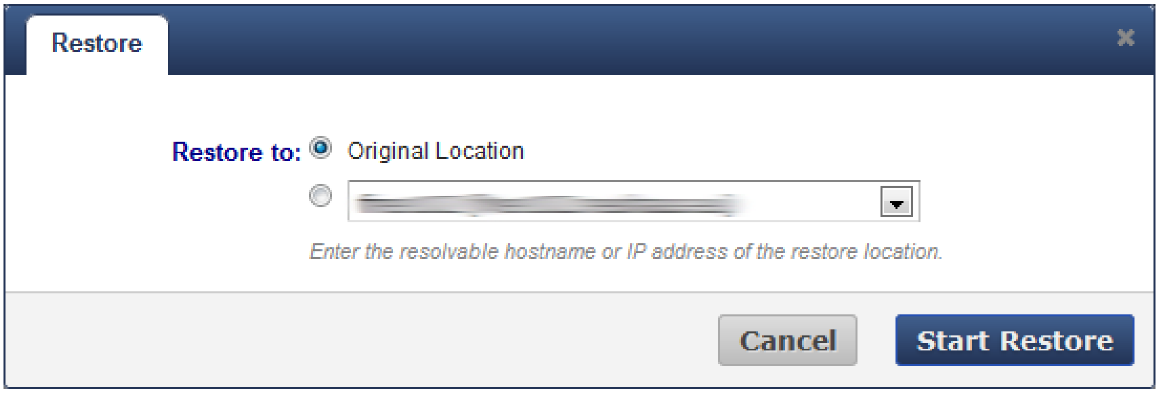
- **Remove the virtual machine** - First shut down and then delete the virtual machine; *or*
- **Keep the original virtual machine** - First clone the virtual machine to assign it a unique identifier (GUID), and then delete the original version of the virtual machine.

Once the virtual machine is removed, you can proceed with restoration.

Restore Data

Use the following steps to restore a Hyper-V virtual machine using Barracuda Backup.

1. Log into the Barracuda Backup web interface, and in the left pane, click on the Barracuda Backup Server from which to restore data.
2. Click **RESTORE**, and in the **Restore Browser** list, click on the Hyper-V source that contains the virtual machine to restore, and click **Restore** to the right of the virtual machine.
3. In the **Restore** dialog box, click **Original Location**:



Restore to: ● Original Location
○
Enter the resolvable hostname or IP address of the restore location.

4. Click **Start Restore.**

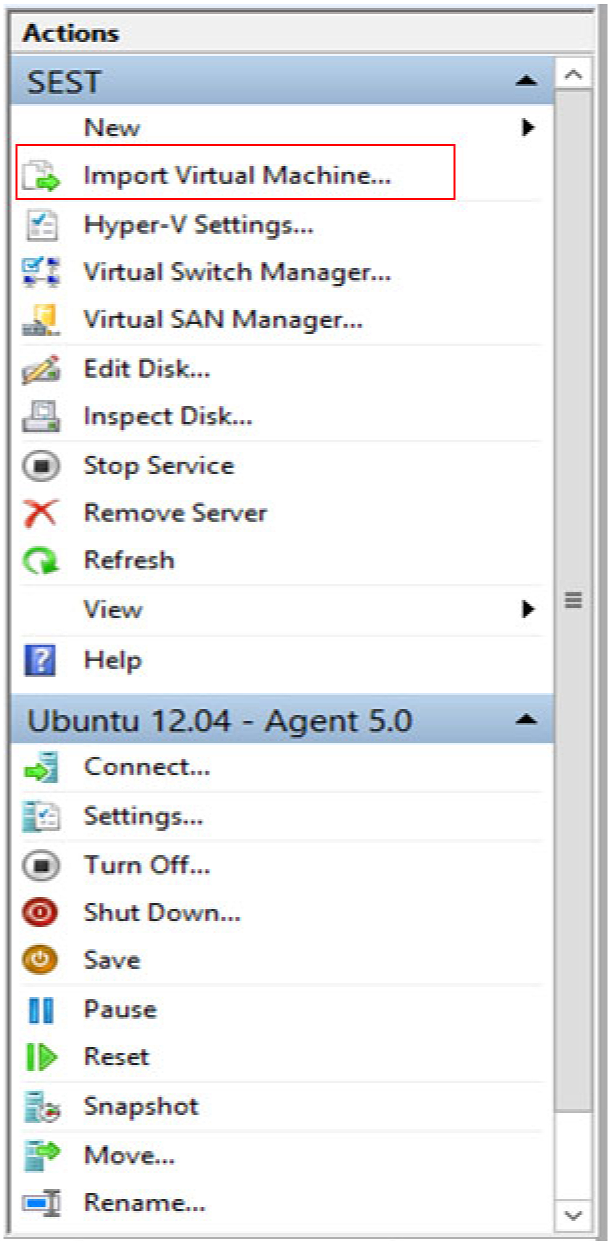
Restore Progress
Go to the **REPORTS > Restore** page to view restore progress.

5. Data is restored to the original location.

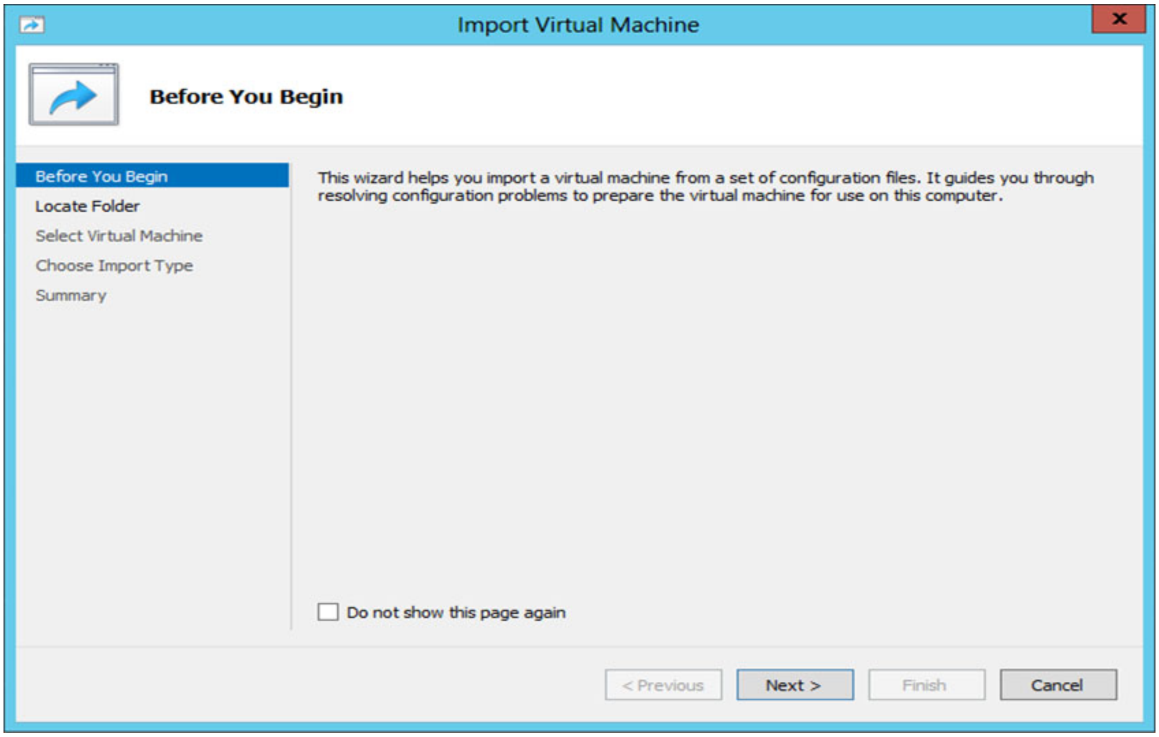
Import the Virtual Machine

Use the following steps to import the virtual machine.

1. Open the Hyper-V Manager, and click **Import Virtual Machine** in the **Actions** pane:


Actions
SEST
New
Import Virtual Machine...
Hyper-V Settings...
Virtual Switch Manager...
Virtual SAN Manager...
Edit Disk...
Inspect Disk...
Stop Service
Remove Server
Refresh
View
Help
Ubuntu 12.04 - Agent 5.0
Connect...
Settings...
Turn Off...
Shut Down...
Save
Pause
Reset
Snapshot
Move...
Rename...

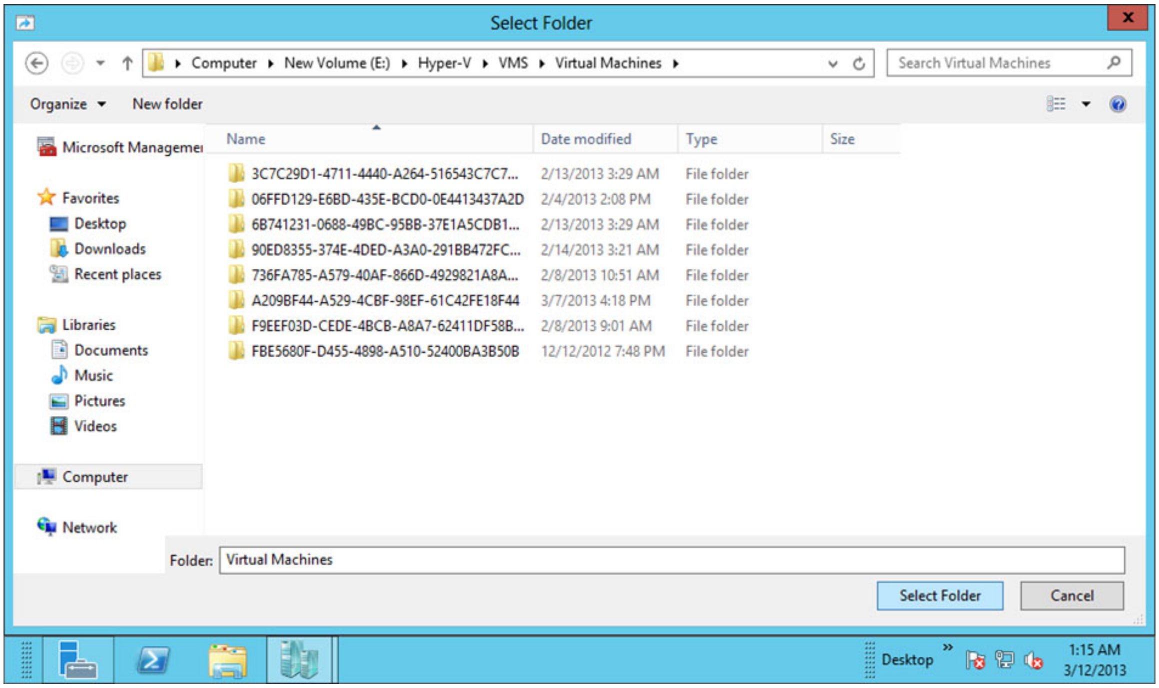
2. In the **Import Virtual Machine** dialog box, click **Next**:


Import Virtual Machine
Before You Begin
Before You Begin
Locate Folder
Select Virtual Machine
Choose Import Type
Summary
< Previous
Next >
Finish
Cancel

This wizard helps you import a virtual machine from a set of configuration files. It guides you through resolving configuration problems to prepare the virtual machine for use on this computer.

☐ Do not show this page again

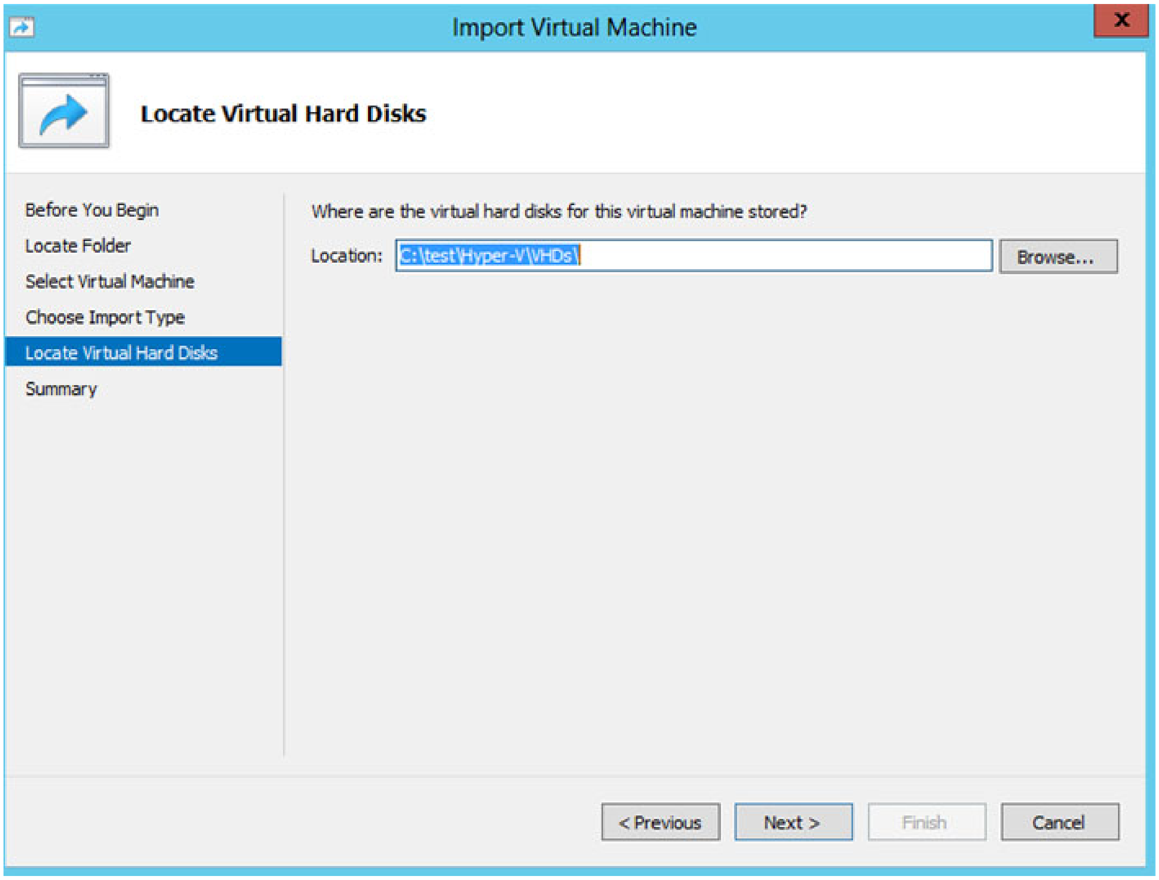
3. Browse to the folder where the virtual machine was restored, and locate the **.vhd** file:


Select Folder
Computer ▸ New Volume (E:) ▸ Hyper-V ▸ VMS ▸ Virtual Machines ▸
Search Virtual Machines
Organize
New folder
Microsoft Manageme
Favorites
Desktop
Downloads
Recent places
Libraries
Documents
Music
Pictures
Videos
Computer
Network
Select Folder
Cancel
Desktop
1:15 AM
3/12/2013

Name	Date modified	Type	Size
3C7C29D1-4711-4440-A264-516543C7C7...	2/13/2013 3:29 AM	File folder	
06FFD129-E6BD-435E-BCD0-0E4413437A2D	2/4/2013 2:08 PM	File folder	
6B741231-0688-49BC-95BB-37E1A5CDB1...	2/13/2013 3:29 AM	File folder	
90ED8355-374E-4DED-A3A0-291BB472FC...	2/14/2013 3:21 AM	File folder	
736FA785-A579-40AF-866D-4929821A8A...	2/8/2013 10:51 AM	File folder	
A209BF44-A529-4CBF-98EF-61C42FE18F44	3/7/2013 4:18 PM	File folder	
F9EEF03D-CEDE-4BCB-A8A7-62411DF58B...	2/8/2013 9:01 AM	File folder	
FBE5680F-D455-4898-A510-52400BA3B50B	12/12/2012 7:48 PM	File folder	

Folder: Virtual Machines

4. Click **Select Folder**. Select the virtual machine to import, and click **Next**.
5. Select the type of import to perform, and click **Next**.
6. Browse to the location of the virtual disks:


Import Virtual Machine
Locate Virtual Hard Disks
Before You Begin
Locate Folder
Select Virtual Machine
Choose Import Type
Locate Virtual Hard Disks
Summary

Where are the virtual hard disks for this virtual machine stored?

Location: C:\test\Hyper-V\VHDs\

Browse...
< Previous
Next >
Finish
Cancel

7. Click **Next**. Click **Finish**, and start your virtual machine.

Microsoft Windows Server Active Directory

In this Section

- How to Restore a Microsoft Server 2012 Active Directory Object from the Active Directory Recycle Bin
- How to Enable Active Directory Recycle Bin on Windows Server 2012
- How to Restore a Microsoft Server 2008 R2 Active Directory Object from the Active Directory Recycle Bin
- How to Enable Active Directory Recycle Bin on Windows Server 2008 R2

How to Restore a Microsoft Server 2012 Active Directory Object from the Active Directory Recycle Bin

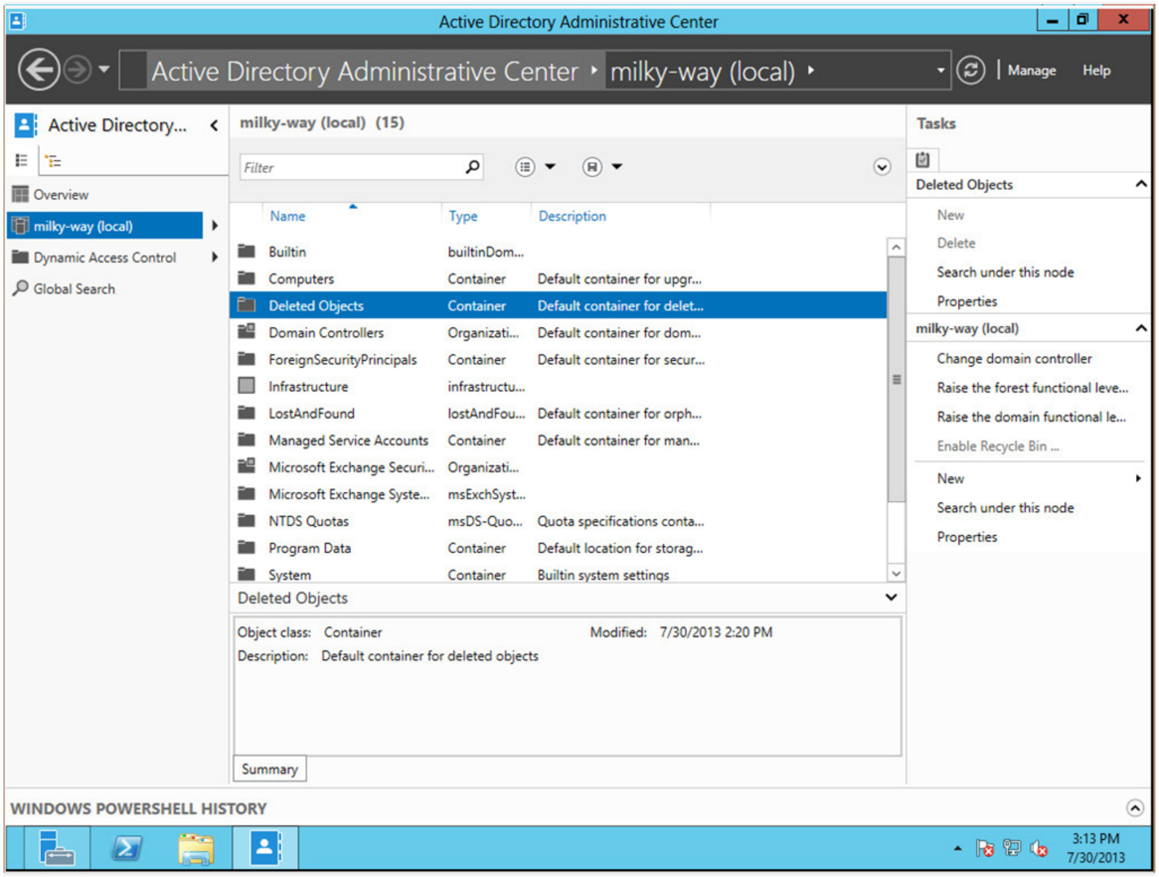
> This article refers to Barracuda Backup firmware version 5.0 or higher, and Microsoft® Active Directory (AD) on Microsoft Windows Server ® 2012.

Related Articles
• Enable AD Recycle Bin on Windows Server 2012 • Restore Microsoft Server 2008 R2 AD Object from AD Recycle Bin • How to Back Up Microsoft Active Directory

Additional Resources
• Restore a Deleted Active Directory Object

Use the following steps to restore an AD Object from the AD Recycle Bin:

1. Log in to the Windows Server 2012 as the administrator.
2. Go to **Start**, and type `dsac.exe` to open the ADAC, or in **Server Manager**, click **Tools**, and then click **Active Directory Administrative Center**.
3. In the left pane, click on the target Server name; a **Deleted Objects** container displays in the center pane:


Active Directory Administrative Center
Active Directory Administrative Center ‣ milky-way (local) ‣
Manage
Help
Active Directory...
Overview
milky-way (local)
Dynamic Access Control
Global Search
milky-way (local) (15)
Filter
Tasks
Deleted Objects
New
Delete
Search under this node
Properties
milky-way (local)
Change domain controller
Raise the forest functional leve...
Raise the domain functional le...
Enable Recycle Bin ...
New
Search under this node
Properties
Summary
WINDOWS POWERSHELL HISTORY
3:13 PM
7/30/2013

Name	Type	Description
Builtin	builtinDom...	
Computers	Container	Default container for upgr...
Deleted Objects	Container	Default container for delet...
Domain Controllers	Organizati...	Default container for dom...
ForeignSecurityPrincipals	Container	Default container for secur...
Infrastructure	infrastructu...	
LostAndFound	lostAndFou...	Default container for orph...
Managed Service Accounts	Container	Default container for man...
Microsoft Exchange Securi...	Organizati...	
Microsoft Exchange Syste...	msExchSyst...	
NTDS Quotas	msDS-Quo...	Quota specifications conta...
Program Data	Container	Default location for storag...
System	Container	Builtin system settings

Deleted Objects

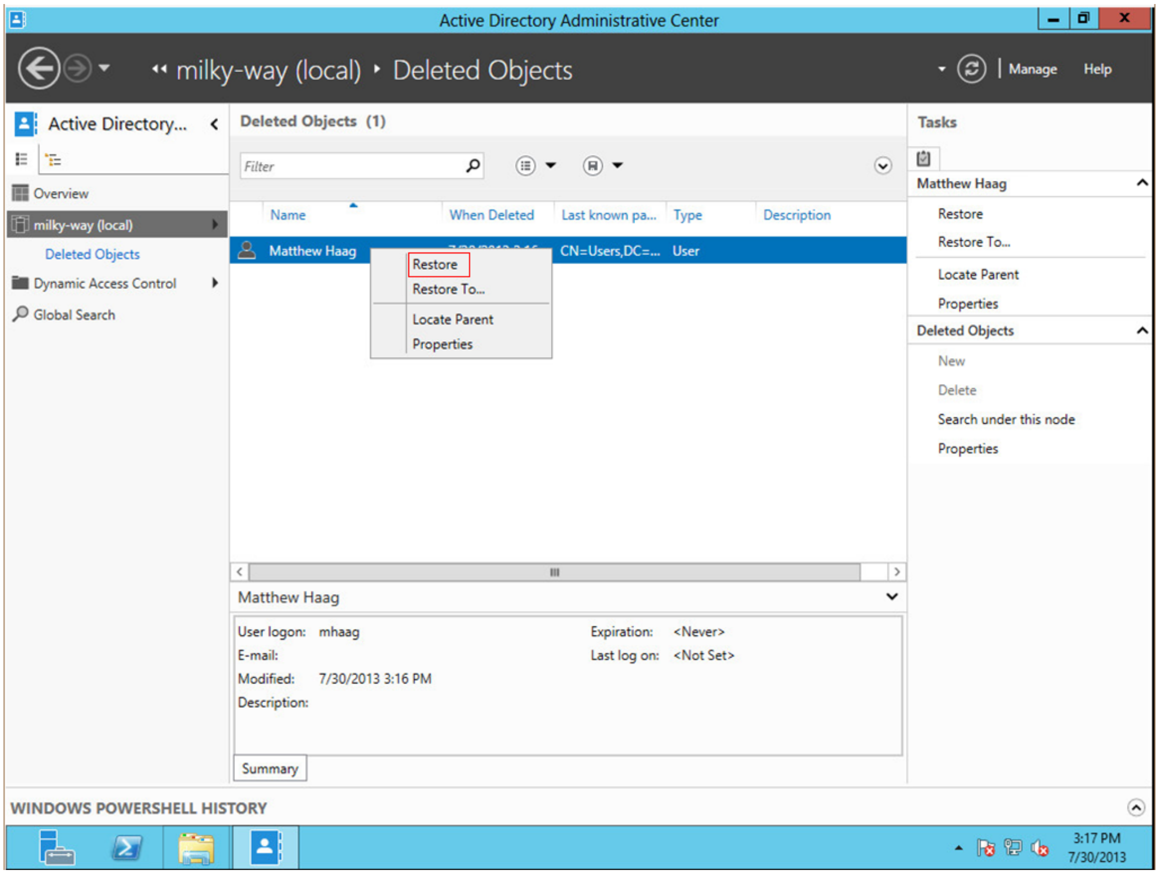
Object class: Container

Modified: 7/30/2013 2:20 PM

Description: Default container for deleted objects

Deleted Objects Container
If the **Deleted Objects** container does not display, right-click on the Server name in the left pane to enable the container.

4. Double-click the **Deleted Objects** container to view a list of deleted items which can be restored.
5. Right-click on the user to restore, and click **Restore**:


Active Directory Administrative Center
milky-way (local) ▸ Deleted Objects
Manage
Help
Active Directory...
Overview
milky-way (local)
Deleted Objects
Dynamic Access Control
Global Search
Deleted Objects (1)
Filter
Name
When Deleted
Last known pa...
Type
Description
Matthew Haag
CN=Users,DC=...
User
Restore
Restore To...
Locate Parent
Properties
Tasks
Matthew Haag
Restore
Restore To...
Locate Parent
Properties
Deleted Objects
New
Delete
Search under this node
Properties
Matthew Haag
Summary
WINDOWS POWERSHELL HISTORY
3:17 PM
7/30/2013

User logon: mhaag
E-mail:
Modified: 7/30/2013 3:16 PM
Description:
Expiration: <Never>
Last log on: <Not Set>

6. Verify the user has been restored.

How to Enable Active Directory Recycle Bin on Windows Server 2012

This article refers to firmware version 5.0 and higher, and Microsoft ® Windows Server ® 2012.

In this article:

- Requirements
- Step 1. Raise the Forest Functional Level
- Step 2. Enable Acitve Directory Recycle Bin

Related Articles

- Restore a Server 2012 Active Directory Object from the Active Directory Recycle Bin
- How to Back Up Microsoft Active Directory
- Enable Active Directory Recycle Bin on Windows Server 2008 R2

Additional Resources

- Active Directory Recycle Bin

⚠ **Warning**
Once you enable Active Directory (AD) Recycle Bin in your environment, you *cannot* disable it.

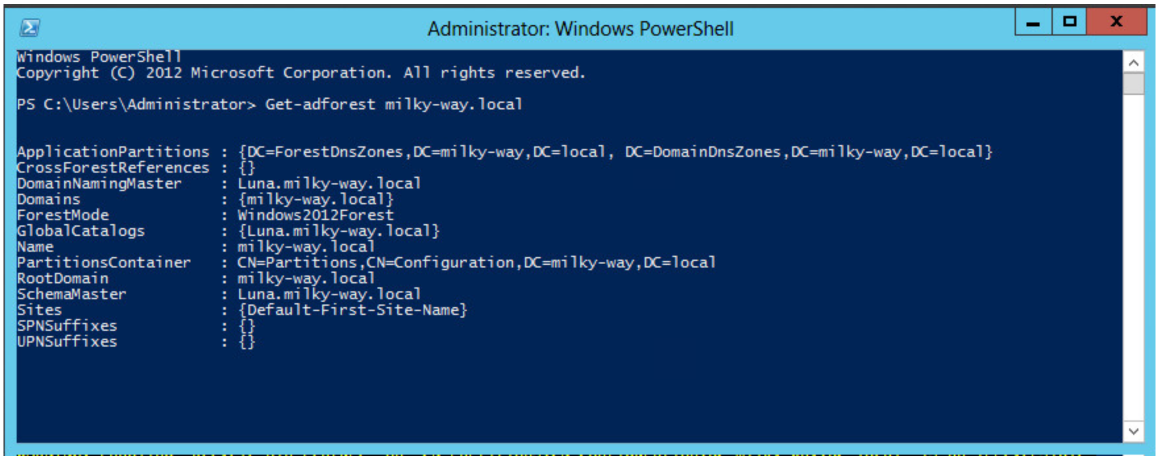
Requirements

To manage the Recycle Bin feature through a user interface, you must install Active Directory Administrative Center in Windows Server 2012.

Step 1. Raise the Forest Functional Level

Before enabling AD Recycle Bin, you must first raise the forest functional level of your AD domain services (DS):

1. Log in to the Windows Server, and open Windows PowerShell.
2. At the PowerShell command prompt, enter the following cmdlet on a single line:
   ```
   Set-ADForestMode -Identity contoso.com -ForestMode Windows2008R2Forest
   -Confirm:$false
   ```
   Where `-Identity` represents the fully qualified DNS name:

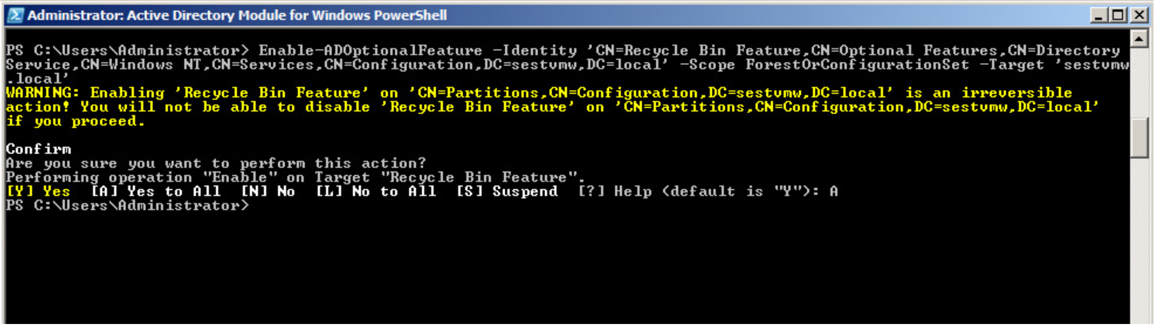


```
Windows PowerShell
Copyright (C) 2012 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Get-adforest milky-way.local


ApplicationPartitions : {DC=ForestDnsZones,DC=milky-way,DC=local, DC=DomainDnsZones,DC=milky-way,DC=local}
CrossForestReferences : {}
DomainNamingMaster    : Luna.milky-way.local
Domains               : {milky-way.local}
ForestMode            : Windows2012Forest
GlobalCatalogs        : {Luna.milky-way.local}
Name                  : milky-way.local
PartitionsContainer   : CN=Partitions,CN=Configuration,DC=milky-way,DC=local
RootDomain            : milky-way.local
SchemaMaster          : Luna.milky-way.local
Sites                 : {Default-First-Site-Name}
SPNSuffixes           : {}
UPNSuffixes           : {}
```

Step 2. Enable Acitve Directory Recycle Bin

Complete the following steps to enable AD Recycle Bin in Active Directory Administrative Center (ADAC) on the target domain:

1. Log in to the Windows Server, and open Windows PowerShell .
2. At the PowerShell command prompt, enter the following command; note that some wrapping may occur due to formatting constraints:
   ```
    Enable-ADOptionalFeature -Identity 'CN=Recycle Bin Feature,CN=Optional
   Features,CN=Directory Service,CN=Windows
   NT,CN=Services,CN=Configuration,DC=contoso,DC=com' -Scope
   ForestOrConfigurationSet -Target 'contoso.com
   ```
3. Press **Enter:**


Administrator: Active Directory Module for Windows PowerShell

```
PS C:\Users\Administrator> Enable-ADOptionalFeature -Identity 'CN=Recycle Bin Feature,CN=Optional Features,CN=Directory
Service,CN=Windows NT,CN=Services,CN=Configuration,DC=sestvmw,DC=local' -Scope ForestOrConfigurationSet -Target 'sestvmw
.local'
WARNING: Enabling 'Recycle Bin Feature' on 'CN=Partitions,CN=Configuration,DC=sestvmw,DC=local' is an irreversible
action! You will not be able to disable 'Recycle Bin Feature' on 'CN=Partitions,CN=Configuration,DC=sestvmw,DC=local'
if you proceed.

Confirm
Are you sure you want to perform this action?
Performing operation "Enable" on Target "Recycle Bin Feature".
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): A
PS C:\Users\Administrator>
```

4. AD Recycle Bin is now enabled.

How to Restore a Microsoft Server 2008 R2 Active Directory Object from the Active Directory Recycle Bin

This article refers to Barracuda Backup firmware version 5.0 or higher, and Microsoft® Active Directory (AD) on Microsoft Windows Server® 2008 R2.

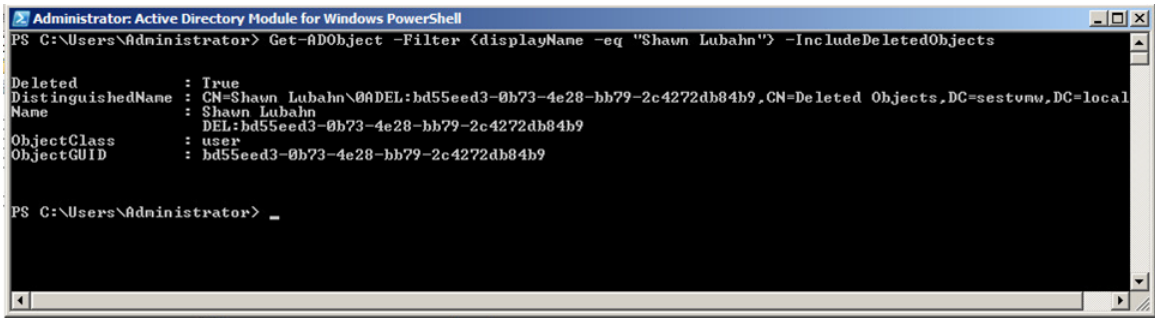
Related Articles
• How to Back Up Microsoft Active Directory

Additional Resources

- Restore a Deleted Active Directory Object

Use the following steps to restore an AD Object from the AD Recycle Bin:

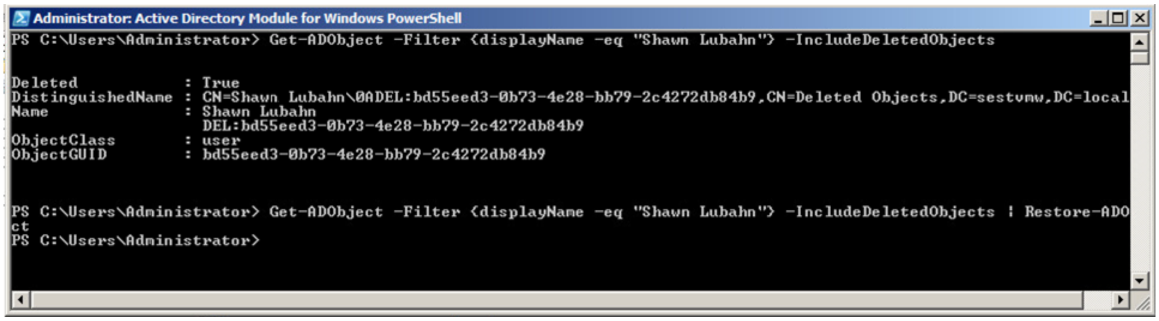
1. Log in to the Windows Server 2008 R2 as the administrator.
2. Go to **Start > Administrative Tools**, right-click **Active Directory Module for WIndows PowerShell**, and click **Run as administrator**.
3. At the command prompt, enter the following command to verify that the object has been deleted:
   `Get-ADObject -Filter {displayName -eq "Shawn Lubahn"} -IncludeDeletedObjects`
   Where `displayName` is the name of the deleted user object:



Administrator: Active Directory Module for Windows PowerShell

```
PS C:\Users\Administrator> Get-ADObject -Filter {displayName -eq "Shawn Lubahn"} -IncludeDeletedObjects


Deleted           : True
DistinguishedName : CN=Shawn Lubahn\0ADEL:bd55eed3-0b73-4e28-bb79-2c4272db84b9,CN=Deleted Objects,DC=sestvmw,DC=local
Name              : Shawn Lubahn
                    DEL:bd55eed3-0b73-4e28-bb79-2c4272db84b9
ObjectClass       : user
ObjectGUID        : bd55eed3-0b73-4e28-bb79-2c4272db84b9



PS C:\Users\Administrator> _
```

4. Press **Enter**.
5. At the command prompt, enter the following command to restore the deleted object:
   `Get-ADObject -Filter {displayName -eq "Shawl Lubahn"} -IncludeDeletedObjects | Restore-ADObject`



Administrator: Active Directory Module for Windows PowerShell

```
PS C:\Users\Administrator> Get-ADObject -Filter {displayName -eq "Shawn Lubahn"} -IncludeDeletedObjects


Deleted           : True
DistinguishedName : CN=Shawn Lubahn\0ADEL:bd55eed3-0b73-4e28-bb79-2c4272db84b9,CN=Deleted Objects,DC=sestvmw,DC=local
Name              : Shawn Lubahn
                    DEL:bd55eed3-0b73-4e28-bb79-2c4272db84b9
ObjectClass       : user
ObjectGUID        : bd55eed3-0b73-4e28-bb79-2c4272db84b9



PS C:\Users\Administrator> Get-ADObject -Filter {displayName -eq "Shawn Lubahn"} -IncludeDeletedObjects | Restore-ADO
ct
PS C:\Users\Administrator>
```

6. Verify the user has been restored.

How to Enable Active Directory Recycle Bin on Windows Server 2008 R2

This article refers to firmware version 5.0 and higher, and Microsoft® Windows Server 2008 R2.

In this article:

- Requirements
- Enable Active Directory Recycle Bin

Related Articles

- How to Enable Active Directory Recycle bin on Windows Server 2012

Additional Resources

- Local and Domain Default Groups
- Enable Active Directory Recycle Bin

Warning
Once you enable Active Directory (AD) Recycle Bin in your environment, you *cannot* disable it.

Requirements

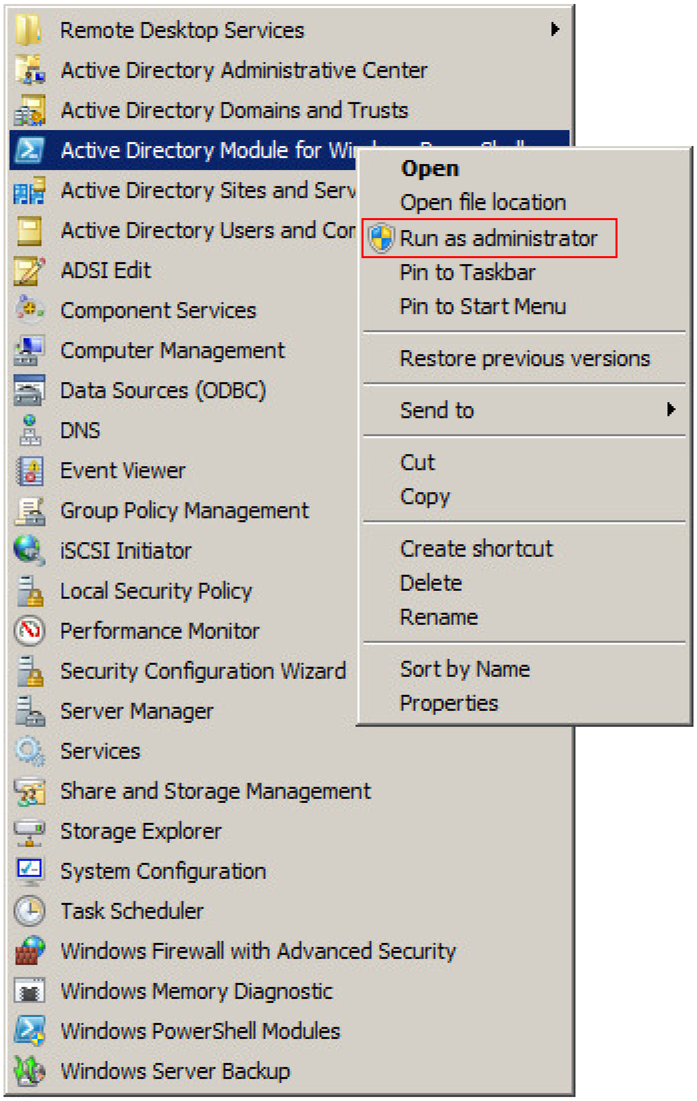
At a minimum, you must have membership in Enterprise Admins, or equivalent access privileges. For additional information, refer to the Microsoft TechNet article Local and Domain Default Groups.

Enable Active Directory Recycle Bin

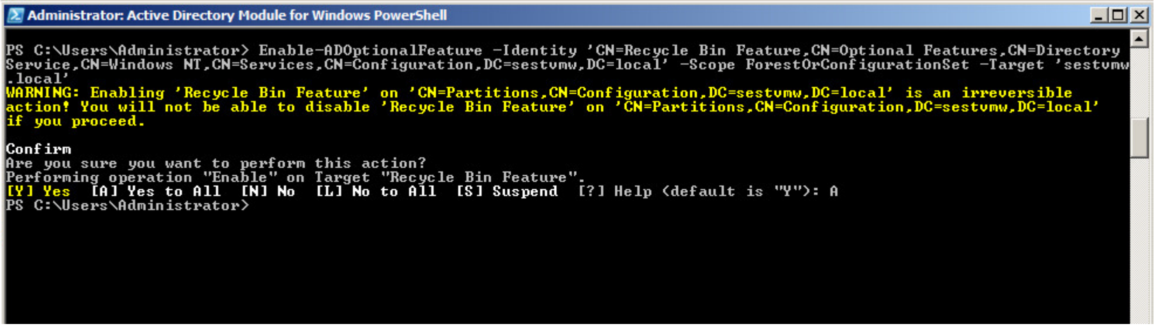
> **Important**
> You must use **Active Directory Module for Windows PowerShell** to run the commands described in this set of steps or an error will occur. To run these commands using Windows PowerShell directly, run the command `import-module activedirectory` to import the Active Directory cmdlet.

Use the following steps to enable AD Recycle Bin using the Enable-ADOptionalFeature cmdlet:

1. Log in to the Windows Server, and go to **Start > Administrative Tools**.
2. Right-click **Active Directory Module for Windows PowerShell**, and click **Run as administrator**:


Remote Desktop Services
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Wi
Active Directory Sites and Serv
Active Directory Users and Cor
ADSI Edit
Component Services
Computer Management
Data Sources (ODBC)
DNS
Event Viewer
Group Policy Management
iSCSI Initiator
Local Security Policy
Performance Monitor
Security Configuration Wizard
Server Manager
Services
Share and Storage Management
Storage Explorer
System Configuration
Task Scheduler
Windows Firewall with Advanced Security
Windows Memory Diagnostic
Windows PowerShell Modules
Windows Server Backup
Open
Open file location
Run as administrator
Pin to Taskbar
Pin to Start Menu
Restore previous versions
Send to
Cut
Copy
Create shortcut
Delete
Rename
Sort by Name
Properties

3. At the PowerShell command prompt, enter the following command, replacing the bracketed variable as appropriate:
   ```
   Enable-ADOptionalFeature -Identity <ADOptionalFeature> -Scope
   <ADOptionalFeatureScope> -Target <ADEntity>
   ```
4. Press **Enter:**



Administrator: Active Directory Module for Windows PowerShell

```
PS C:\Users\Administrator> Enable-ADOptionalFeature -Identity 'CN=Recycle Bin Feature,CN=Optional Features,CN=Directory
Service,CN=Windows NT,CN=Services,CN=Configuration,DC=sestvmw,DC=local' -Scope ForestOrConfigurationSet -Target 'sestvmw
.local'
WARNING: Enabling 'Recycle Bin Feature' on 'CN=Partitions,CN=Configuration,DC=sestvmw,DC=local' is an irreversible
action! You will not be able to disable 'Recycle Bin Feature' on 'CN=Partitions,CN=Configuration,DC=sestvmw,DC=local'
if you proceed.

Confirm
Are you sure you want to perform this action?
Performing operation "Enable" on Target "Recycle Bin Feature".
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): A
PS C:\Users\Administrator>
```

5. AD Recycle Bin is now enabled.

Barracuda LiveBoot in the Cloud

Use Barracuda LiveBoot to boot VMware virtual guest systems in the Barracuda Cloud. LiveBoot in the cloud is useful as a sandbox for testing purposes.

In this Section

- Understanding Cloud LiveBoot
- How to Use Barracuda LiveBoot in the Cloud
- How to vMotion a LiveBooted Virtual Machine from the Barracuda Backup Server

Related Articles

How to Restore VMware Guest Systems Using Barracuda LiveBoot

Understanding Cloud LiveBoot

This article refers to firmware 5.0 and higher, and VMware® ESX/ESXi with the VMware license which includes access to vSphere® Data Recovery API.

Cloud LiveBoot™ is available to all Barracuda Backup customers with Instant Replacement and a Cloud storage subscription, and is available to all customers excluding those in Japan, Germany, and Austria.

In this article:

- Virtual Machine States
- Recover and Test Virtual Servers

Related Articles

- How to Use Barracuda LiveBoot in the Cloud
- How to vMotion a LiveBooted Virtual Machine from the Barracuda Backup Server
- How to Restore VMware Guest Systems Using Barracuda LiveBoot

Virtual Machine States

A virtual machine (VM) has three basic states: running, suspend/resume, and stopped. You suspend a VM to save its current state, and then when it is resumed, applications running before it was suspended resume in their running state, content is unchanged, and user session is active. When a VM is stopped, applications are stopped and user sessions are inactive.

Recover and Test Virtual Servers

Cloud LiveBoot allows you to boot VMware virtual guest systems in Barracuda's Cloud for recovery and testing, as described in Table 1.

Table 1. LiveBoot Recovery and Testing Features.

Recovery	- Recover any revision of a VMware virtual guest server within your retention policy. - Boot virtual servers in the cloud to recover and traverse the file structure of VMware virtual guest system data. - Retrieve an individual Active Directory (AD) object. ⓘ **Exporting AD Files** For details on exporting an AD object, refer to the Microsoft TechNet article Import or Export Directory Objects Using Ldifde. - Serve up deduplicated content as needed by the virtual server.
Testing	- Once replicated to the cloud, boot the virtual guest system to verify data integrity. - Use LiveBoot to set up a sandbox to test applications or changes to applications outside of your production environment.

When you back up a VMware virtual guest server and replicate this data to Barracuda Cloud Storage, you can boot the server in Barracuda's Cloud directly from the Barracuda Backup web interface; no additional configuration is necessary. Go to **RESTORE > Restore Browser**, and click **LiveBoot** to the right of the guest server. Allow the operating system to complete the boot process; typically this process takes less than a minute. Once the system is available in the cloud, you are presented your login credentials so that you can use a Virtual Network Computing (VNC) client to connect securely to your guest machine. For direct access, you can connect remotely over a public IP address by modifying the Network Settings to **External**. Note that you must first shutdown the server to enable a public IP address. The public address is allocated by Barracuda.

> ⓘ When accessing a guest machine remotely, because it is assigned a public IP address, you are responsible for securing the virtual machine in the Cloud.

Once a virtual guest is running in the Cloud, it remains operational for seven days; if you require additional time, contact Barracuda Networks Technical Support. The number of virtual images you can run is based on your Barracuda Backup model, as shown in Table 2.

Table 2. VMware Virtual Images by Model.

Model	Available Virtual Images
190/390	1
490/690	3
890/891/892/990/991/1090/1091	5

How to Use Barracuda LiveBoot in the Cloud

> This article refers to firmware 5.2 and higher, and VMware® 4.0 and above.
>
> Use Barracuda LiveBoot to boot VMware virtual guest systems in the Barracuda Cloud. LiveBoot in the cloud is useful as a sandbox for testing purposes.

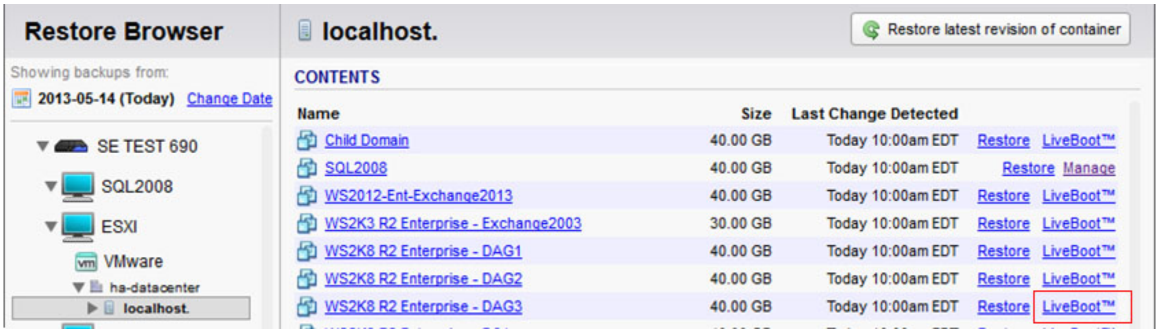
In this article:

- LiveBoot a VMware Virtual Machine from the Cloud
- Connect to your LiveBooted Virtual Machine
- Manage LiveBooted Virtual Machines
- Change the Virtual Machine IP Address
- Download the VMDK File

LiveBoot a VMware Virtual Machine from the Cloud

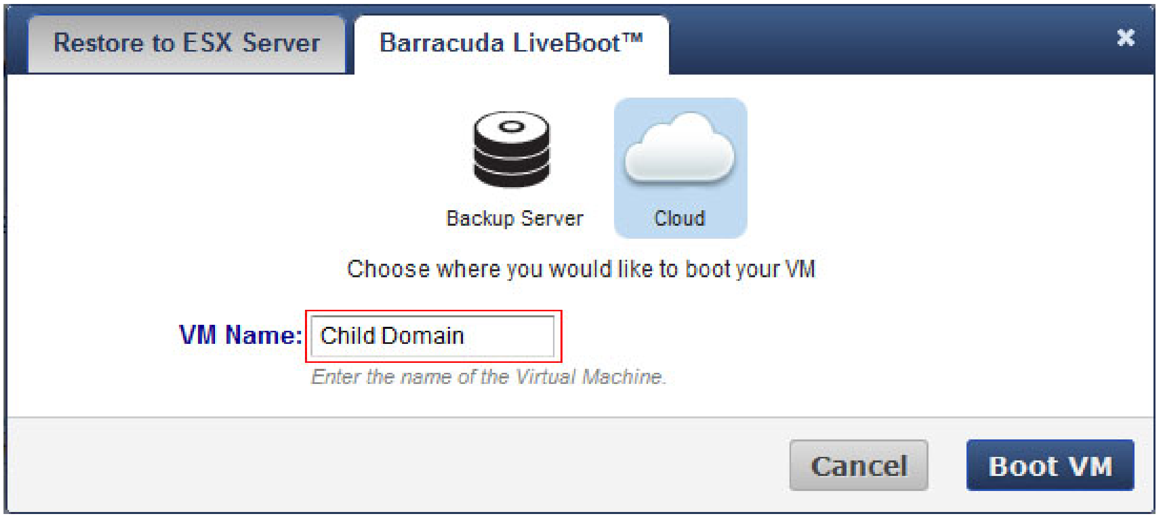
Use the following steps to LiveBoot a VMware virtual machine:

1. Log in to the Barracuda Backup web interface, and go to the **RESTORE** page.
2. Navigate to and expand the VMware Server, click on the guest system you wish to LiveBoot, and click on **LiveBoot** to the right of the system:


Restore Browser
Showing backups from:
2013-05-14 (Today) Change Date
SE TEST 690
SQL2008
ESXI
VMware
ha-datacenter
localhost.
localhost.
Restore latest revision of container
CONTENTS

Name	Size	Last Change Detected		
Child Domain	40.00 GB	Today 10:00am EDT	Restore	LiveBoot™
SQL2008	40.00 GB	Today 10:00am EDT	Restore	Manage
WS2012-Ent-Exchange2013	40.00 GB	Today 10:00am EDT	Restore	LiveBoot™
WS2K3 R2 Enterprise - Exchange2003	30.00 GB	Today 10:00am EDT	Restore	LiveBoot™
WS2K8 R2 Enterprise - DAG1	40.00 GB	Today 10:00am EDT	Restore	LiveBoot™
WS2K8 R2 Enterprise - DAG2	40.00 GB	Today 10:00am EDT	Restore	LiveBoot™
WS2K8 R2 Enterprise - DAG3	40.00 GB	Today 10:00am EDT	Restore	LiveBoot™

3. The dialog box displays the **Barracuda LiveBoot** page; click the **Cloud** icon, and enter a name for the virtual machine in the **VM Name** field:

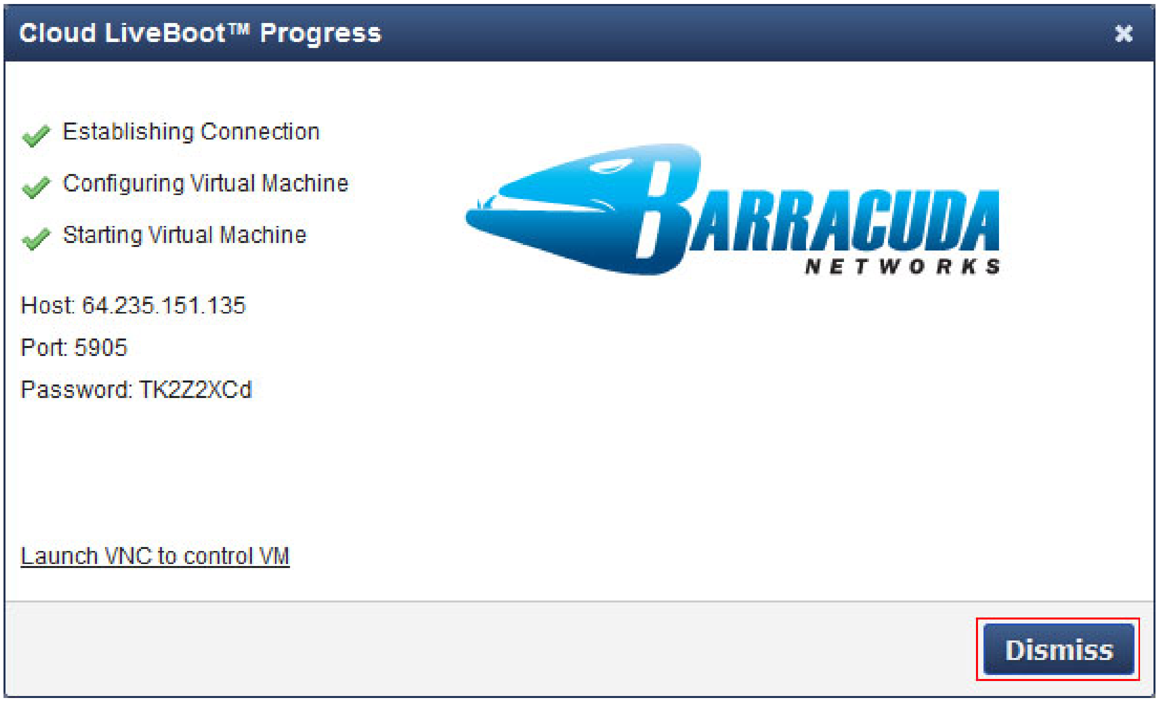

Restore to ESX Server
Barracuda LiveBoot™
Backup Server
Cloud
Cancel
Boot VM

Choose where you would like to boot your VM

VM Name: Child Domain

Enter the name of the Virtual Machine.

4. Click **Boot VM**.
5. The LiveBoot progress dialog box displays; click **Dismiss** to close the dialog; the LiveBoot process is complete:


Cloud LiveBoot™ Progress
BARRACUDA
NETWORKS
Dismiss

✓ Establishing Connection
✓ Configuring Virtual Machine
✓ Starting Virtual Machine

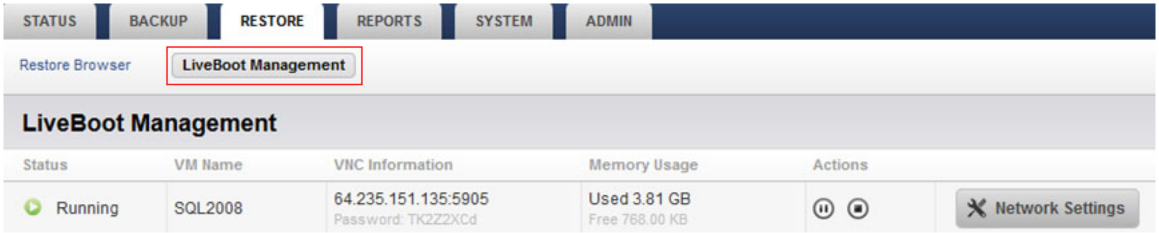
Host: 64.235.151.135
Port: 5905
Password: TK2Z2XCd

Launch VNC to control VM

Connect to your LiveBooted Virtual Machine

You can use a Virtual Network Computing (VNC) client to connect directly to a virtual machine LiveBooted to the cloud:

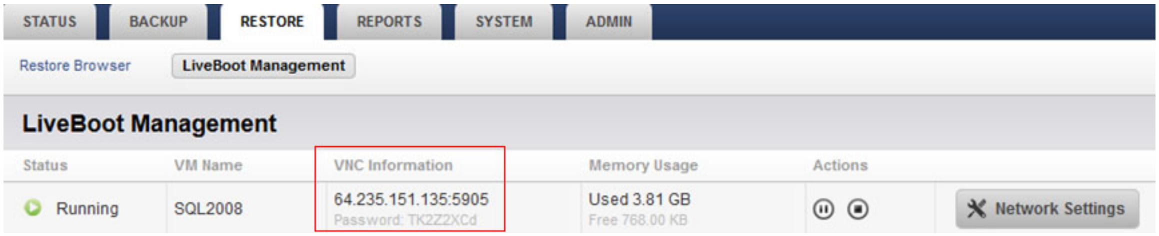
1. To manage your LiveBooted virtual machine, in the **RESTORE** page, click **LiveBoot Management**:


STATUS
BACKUP
RESTORE
REPORTS
SYSTEM
ADMIN
Restore Browser
LiveBoot Management
Network Settings

LiveBoot Management

Status	VM Name	VNC Information	Memory Usage	Actions
Running	SQL2008	64.235.151.135:5905 Password: TK2Z2XCd	Used 3.81 GB Free 768.00 KB	Network Settings

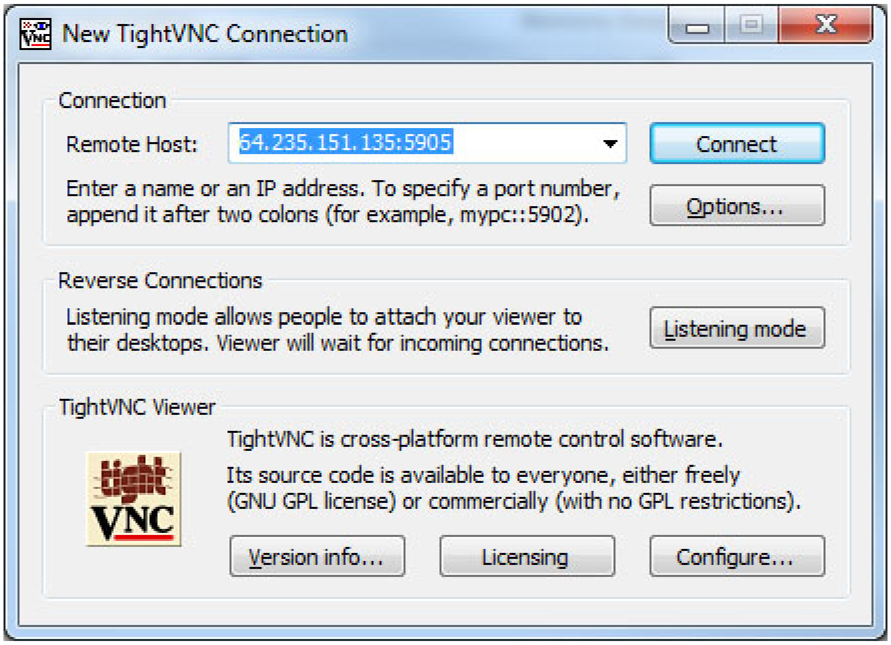
2. The **VNC Information** details display in the table:


STATUS
BACKUP
RESTORE
REPORTS
SYSTEM
ADMIN
Restore Browser
LiveBoot Management
Network Settings

LiveBoot Management

Status	VM Name	VNC Information	Memory Usage	Actions
Running	SQL2008	64.235.151.135:5905 Password: TK2Z2XCd	Used 3.81 GB Free 768.00 KB	Network Settings

3. Open a VNC client, for example, TightVNC, and enter the **VNC Information** from the **RESTORE** page in the **Remote Host** field:


Connect
Options...
Listening mode
Version info...
Licensing
Configure...

New TightVNC Connection

Connection

Remote Host: 64.235.151.135:5905

Enter a name or an IP address. To specify a port number, append it after two colons (for example, mypc::5902).

Reverse Connections

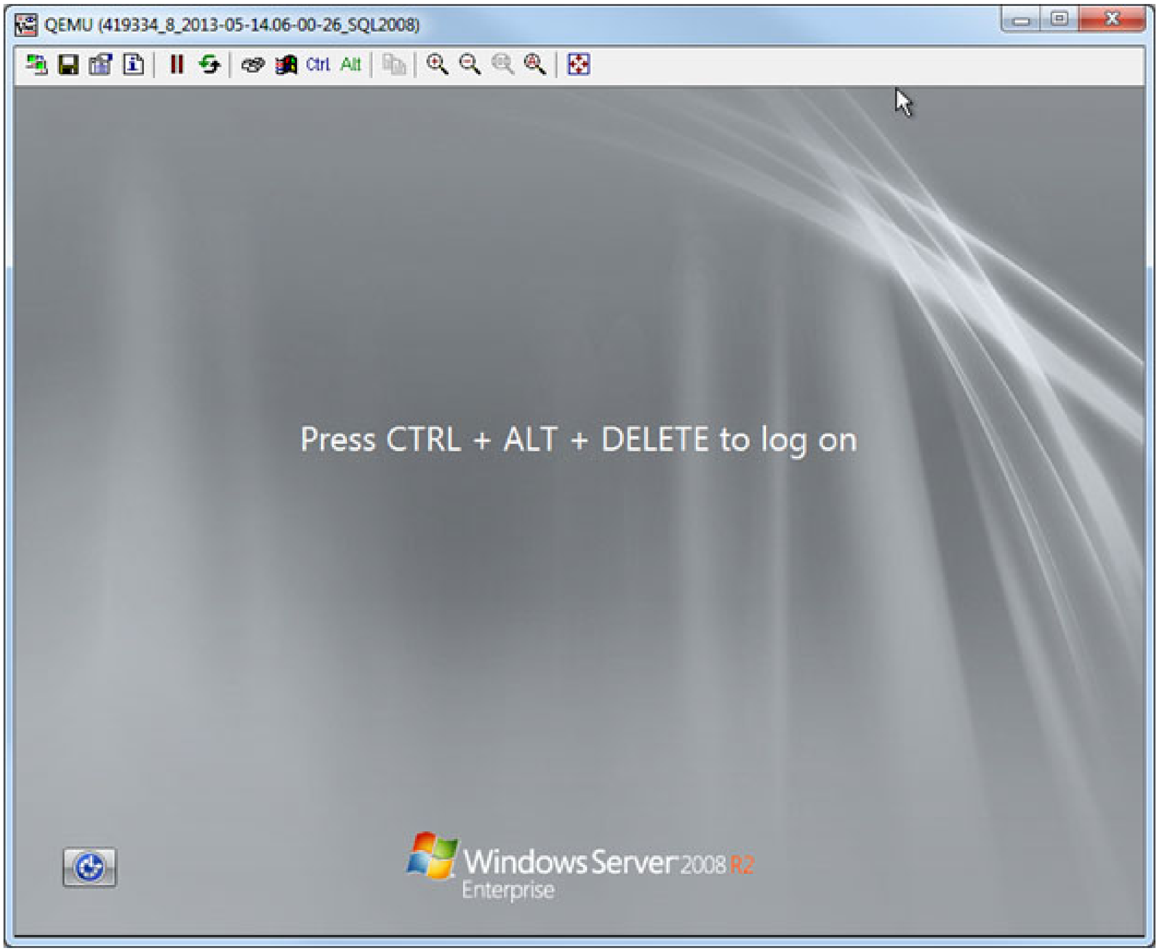
Listening mode allows people to attach your viewer to their desktops. Viewer will wait for incoming connections.

TightVNC Viewer

TightVNC is cross-platform remote control software.

Its source code is available to everyone, either freely (GNU GPL license) or commercially (with no GPL restrictions).

4. Click **Connect**. You should now be connected to your virtual machine LiveBooted from the cloud:


QEMU (419334_8_2013-05-14.06-00-26_SQL2008)
Ctrl
Alt
Windows Server 2008 R2
Enterprise

Press CTRL + ALT + DELETE to log on

Manage LiveBooted Virtual Machines

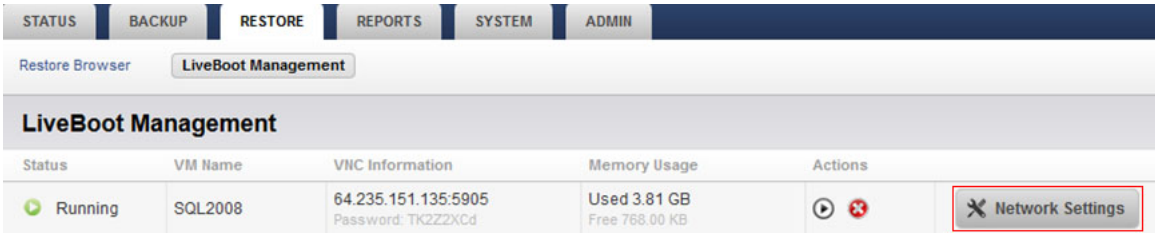
Use the options in the **Actions** column of the **LiveBoot Management** table to manage your LiveBooted virtual machines:

- **Pause** (⏸) icon - Click to pause the virtual machine
- **Play** (▶) icon - Click to restart the virtual machine
- **Shutdown** (⏹) icon - Click to shut down the virtual machine
- **Destroy** (✖) icon - Once you shut down a virtual machine, click this icon to destroy the virtual machine

Change the Virtual Machine IP Address

By default the virtual machine uses a private IP address with no Internet access. If you wish to do so, you can change the address to a public IP address using the following steps:

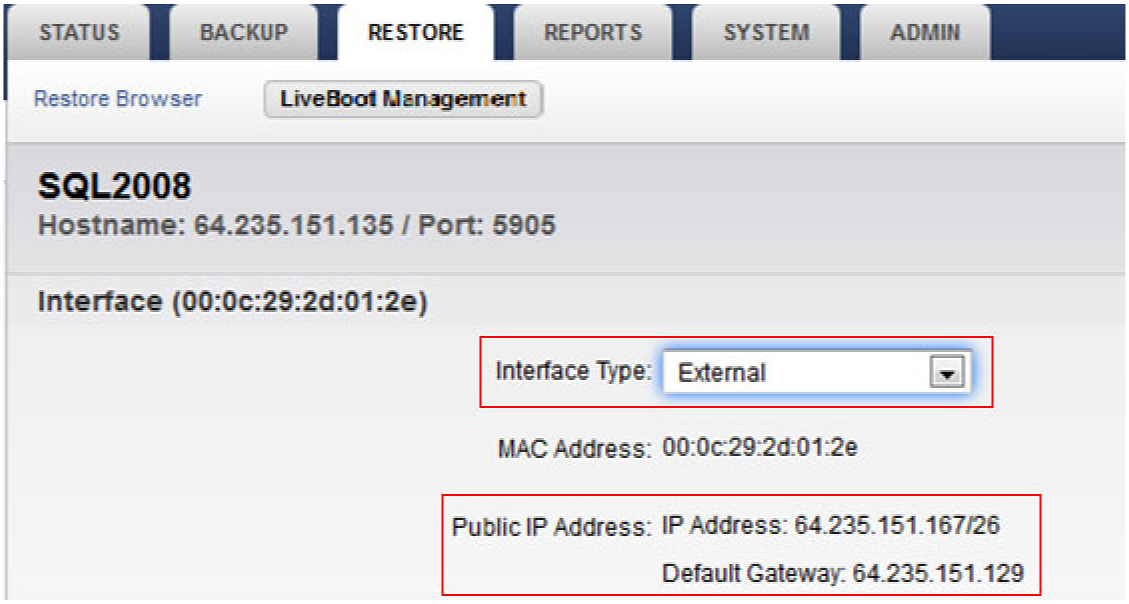
1. In the **LiveBoot Management** table, click the **Shutdown** (⏹) icon in the **Actions** column; the icon changes to the **Destroy** (✖) icon.
2. Click **Network Settings**:


STATUS
BACKUP
RESTORE
REPORTS
SYSTEM
ADMIN
Restore Browser
LiveBoot Management
Network Settings

LiveBoot Management

Status	VM Name	VNC Information	Memory Usage	Actions
Running	SQL2008	64.235.151.135:5905 Password: TK2Z2XCd	Used 3.81 GB Free 768.00 KB	▶ ✖ Network Settings

3. In the **Interface** section, select **External** from the **Interface Type** drop-down menu, and make note of the **Public IP Address** and **Default Gateway** fields (you will need these values to complete **Step 7**):


STATUS
BACKUP
RESTORE
REPORTS
SYSTEM
ADMIN
Restore Browser
LiveBoot Management

SQL2008

Hostname: 64.235.151.135 / Port: 5905

Interface (00:0c:29:2d:01:2e)

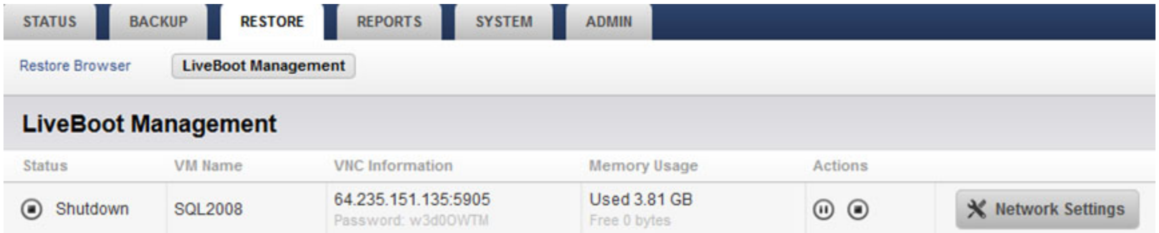
Interface Type: External

MAC Address: 00:0c:29:2d:01:2e

Public IP Address: IP Address: 64.235.151.167/26

Default Gateway: 64.235.151.129

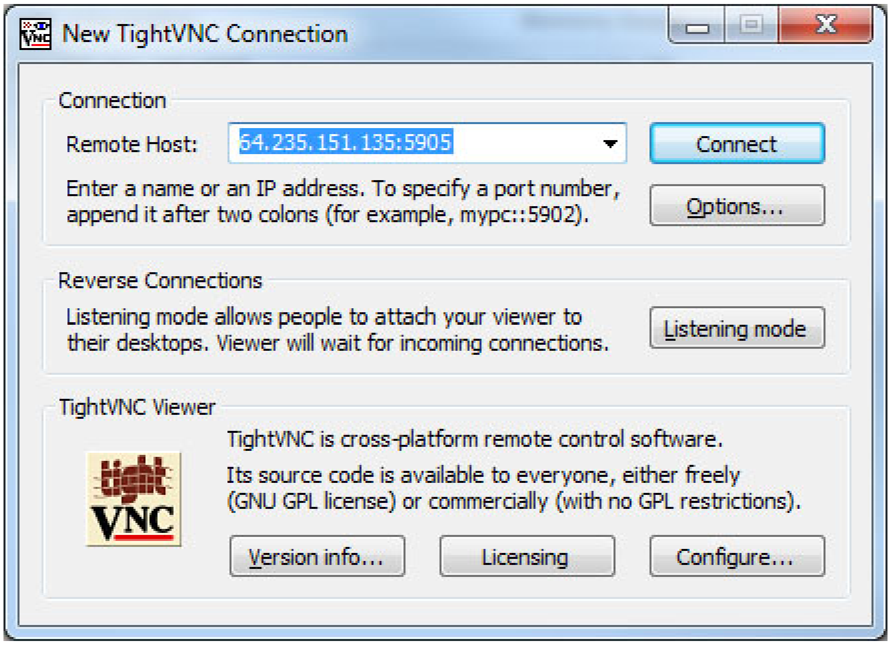
4. Click **LiveBoot Management** at the top of the page, and then click the **Play** (▶) icon in the **Actions** table to start the virtual machine:


STATUS
BACKUP
RESTORE
REPORTS
SYSTEM
ADMIN
Restore Browser
LiveBoot Management
Network Settings

LiveBoot Management

Status	VM Name	VNC Information	Memory Usage	Actions
● Shutdown	SQL2008	64.235.151.135:5905 Password: w3d0OWTM	Used 3.81 GB Free 0 bytes	⏸ ●

5. Open the VNC client again, and connect to the virtual machine:


New TightVNC Connection
Connect
Options...
Listening mode
Version info...
Licensing
Configure...
tight VNC

Connection

Remote Host: 64.235.151.135:5905

Enter a name or an IP address. To specify a port number, append it after two colons (for example, mypc::5902).

Reverse Connections

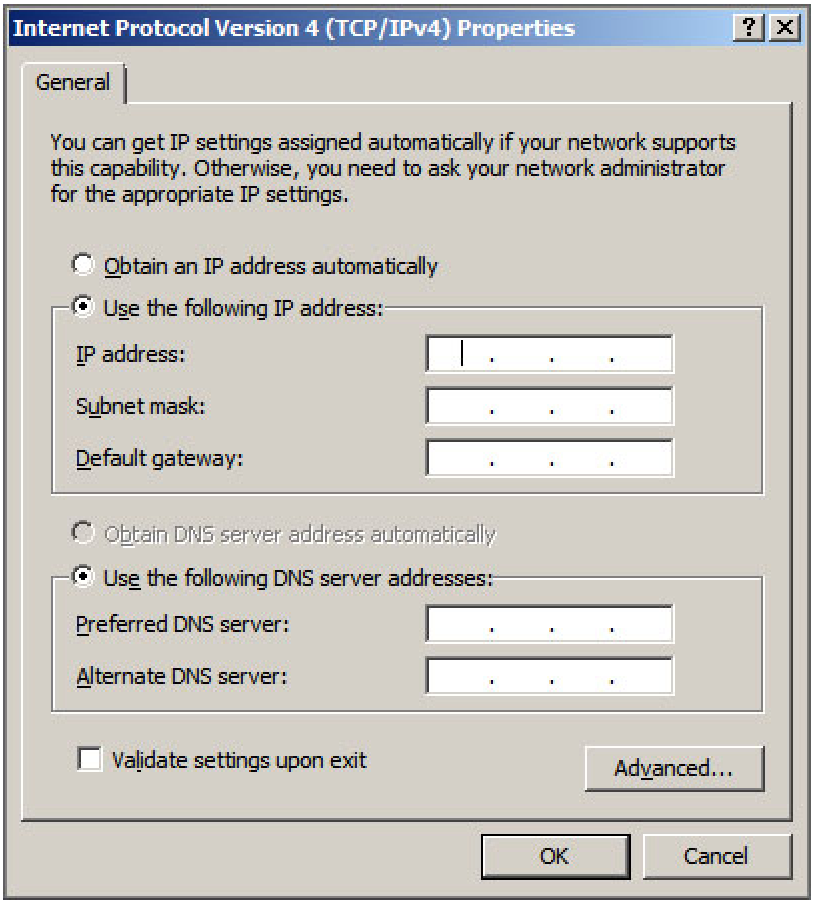
Listening mode allows people to attach your viewer to their desktops. Viewer will wait for incoming connections.

TightVNC Viewer

TightVNC is cross-platform remote control software.

Its source code is available to everyone, either freely (GNU GPL license) or commercially (with no GPL restrictions).

6. Log in to the virtual machine, and open **TCP/IPv4 Properties**:


Internet Protocol Version 4 (TCP/IPv4) Properties
?
General
OK
Cancel
Advanced...

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

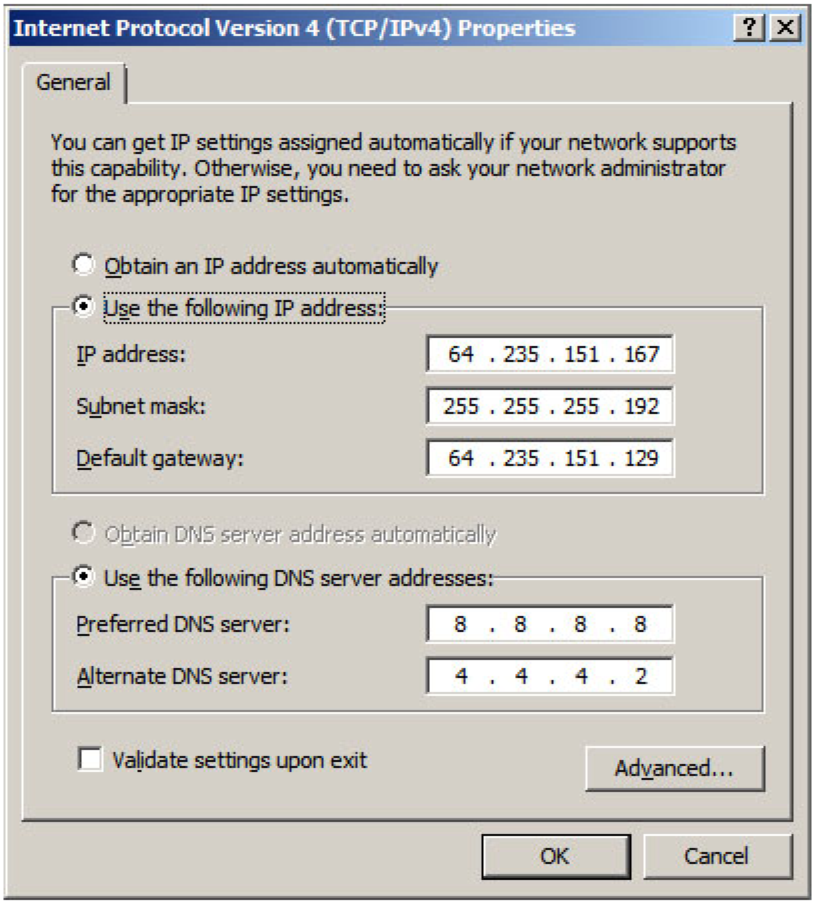
Preferred DNS server: . . .

Alternate DNS server: . . .

☐ Validate settings upon exit

7. Enter the Public IP address values from **Step 3** in to the associated fields; You can use public DNS server values such as 8.8.8.8 and 4.4.4.2:

> You may need a subnet calculator to calculate the subnet mask.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:
IP address: 64 . 235 . 151 . 167
Subnet mask: 255 . 255 . 255 . 192
Default gateway: 64 . 235 . 151 . 129

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: 8 . 8 . 8 . 8
Alternate DNS server: 4 . 4 . 4 . 2

☐ Validate settings upon exit

8. Click **OK** to apply your settings. Open a web browser and confirm that you can connect to the Internet.

> Two virtual machines LiveBooted in the cloud can communicate with each other provided they are both on the same account. Note that each account is assigned a VLAN. The same is true if the virtual machines have a public IP address.

Download the VMDK File

Use the following steps to download the VMDK file:

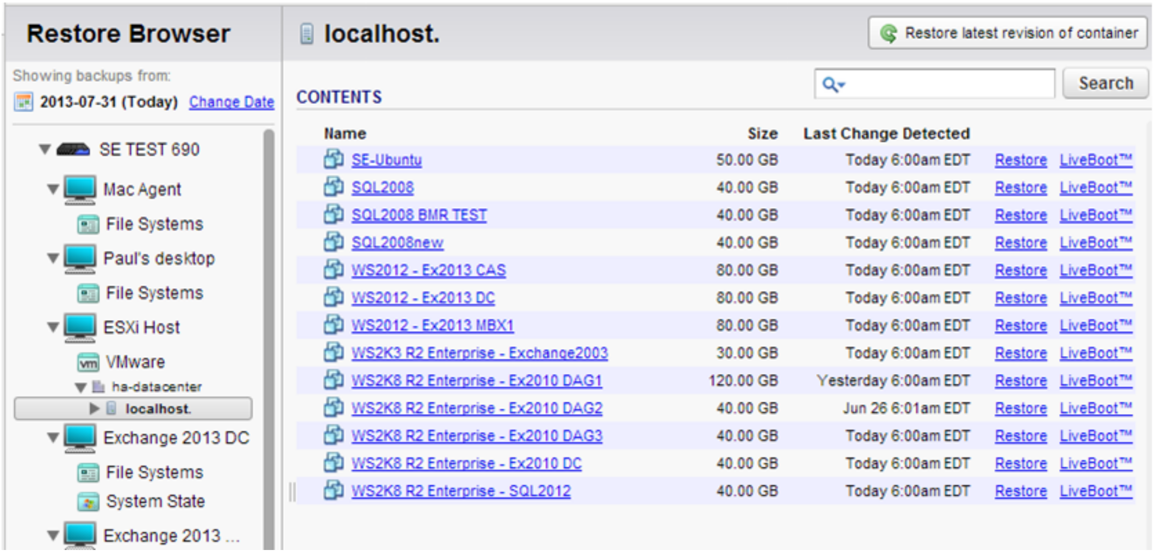
1. Log in to VMware and stop the virtual guest machine.
2. In the Barracuda Backup web interface, go to the **RESTORE > LiveBoot Management** tab.
3. Verify the virtual guest machine **Status** displays as **Shutdown**.
4. Click the **Download** link to download the VMDK file to your local system.

How to vMotion a LiveBooted Virtual Machine from the Barracuda Backup Server

> This article applies to Barracuda Backup firmware version 5.2 and higher, and vmWare® vCenter vSphere vMotion.

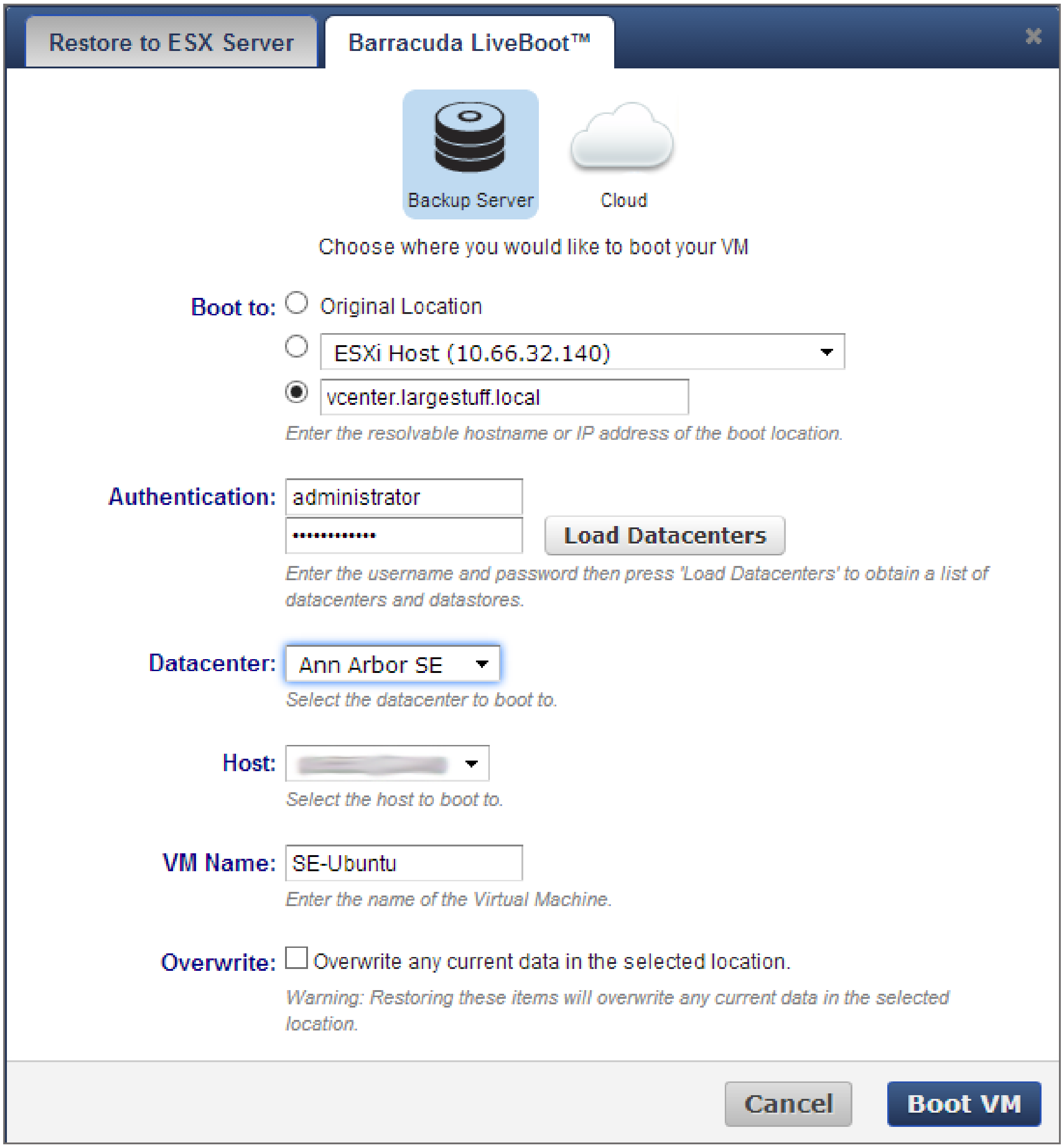
Use the following steps to LiveBoot and vMotion a virtual machine from Barracuda Backup:

1. Log in to Barracuda Backup web interface or the local UI.
2. Go to the **RESTORE > Restore Browser** page, and select the vCenter or host in the left pane.
3. Navigate to and select the virtual machine you want to LiveBoot:


Restore Browser
Showing backups from:
2013-07-31 (Today) Change Date
SE TEST 690
Mac Agent
File Systems
Paul's desktop
File Systems
ESXi Host
VMware
ha-datacenter
localhost.
Exchange 2013 DC
File Systems
System State
Exchange 2013 ...
localhost.
Restore latest revision of container
CONTENTS
Search

Name	Size	Last Change Detected		
SE-Ubuntu	50.00 GB	Today 6:00am EDT	Restore	LiveBoot™
SQL2008	40.00 GB	Today 6:00am EDT	Restore	LiveBoot™
SQL2008 BMR TEST	40.00 GB	Today 6:00am EDT	Restore	LiveBoot™
SQL2008new	40.00 GB	Today 6:00am EDT	Restore	LiveBoot™
WS2012 - Ex2013 CAS	80.00 GB	Today 6:00am EDT	Restore	LiveBoot™
WS2012 - Ex2013 DC	80.00 GB	Today 6:00am EDT	Restore	LiveBoot™
WS2012 - Ex2013 MBX1	80.00 GB	Today 6:00am EDT	Restore	LiveBoot™
WS2K3 R2 Enterprise - Exchange2003	30.00 GB	Today 6:00am EDT	Restore	LiveBoot™
WS2K8 R2 Enterprise - Ex2010 DAG1	120.00 GB	Yesterday 6:00am EDT	Restore	LiveBoot™
WS2K8 R2 Enterprise - Ex2010 DAG2	40.00 GB	Jun 26 6:01am EDT	Restore	LiveBoot™
WS2K8 R2 Enterprise - Ex2010 DAG3	40.00 GB	Today 6:00am EDT	Restore	LiveBoot™
WS2K8 R2 Enterprise - Ex2010 DC	40.00 GB	Today 6:00am EDT	Restore	LiveBoot™
WS2K8 R2 Enterprise - SQL2012	40.00 GB	Today 6:00am EDT	Restore	LiveBoot™

4. Click **LiveBoot** to the right of the virtual machine.
5. In the **Barracuda LiveBoot** dialog box, select either **Original Location** or an alternate location, and enter the virtual machine details:


Restore to ESX Server
Barracuda LiveBoot™
Backup Server
Cloud

Choose where you would like to boot your VM

Boot to: ○ Original Location

○ ESXi Host (10.66.32.140)

● vcenter.largestuff.local

Enter the resolvable hostname or IP address of the boot location.

Authentication: administrator

••••••••••••

Enter the username and password then press 'Load Datacenters' to obtain a list of datacenters and datastores.

Datacenter: Ann Arbor SE

Select the datacenter to boot to.

Host:

Select the host to boot to.

VM Name: SE-Ubuntu

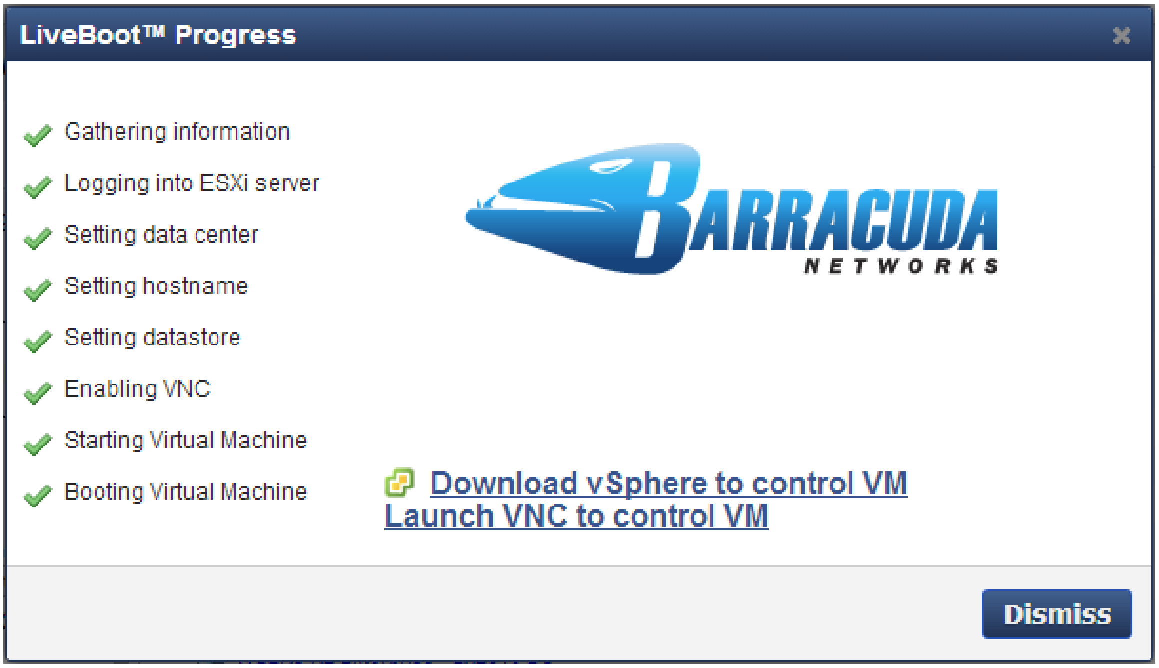
Enter the name of the Virtual Machine.

Overwrite: ☐ Overwrite any current data in the selected location.

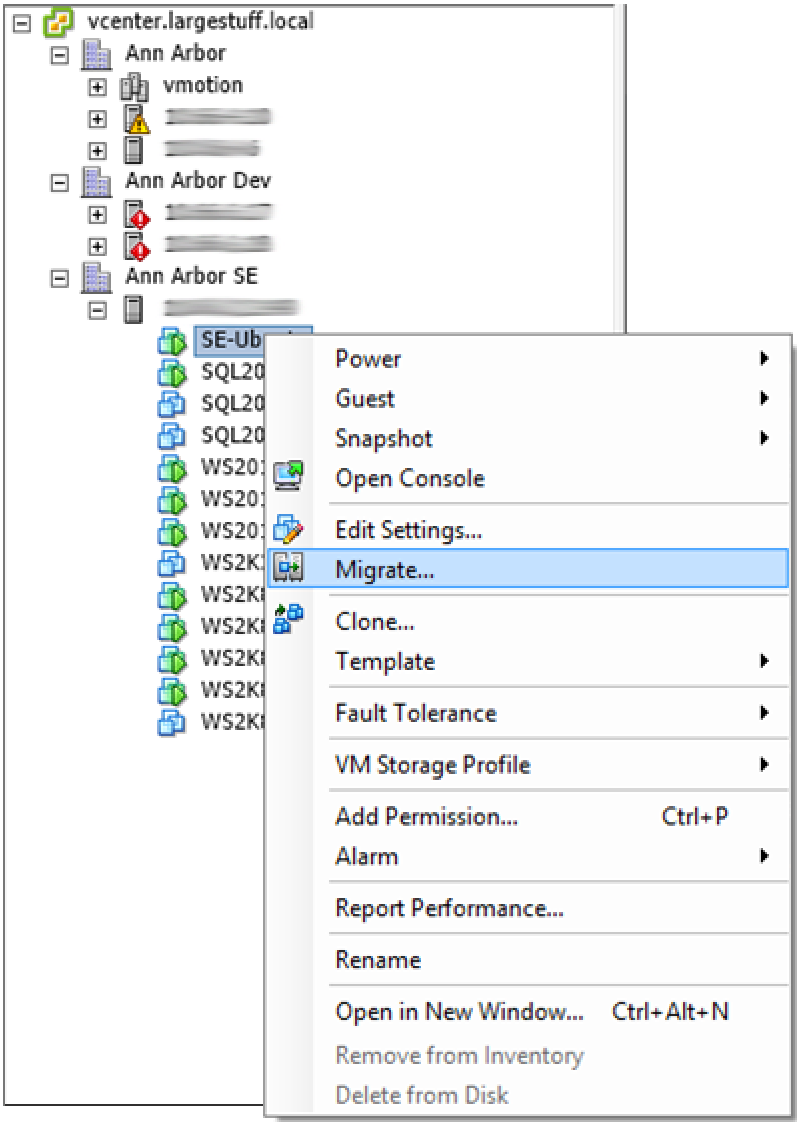
Warning: Restoring these items will overwrite any current data in the selected location.

Load Datacenters
Cancel
Boot VM

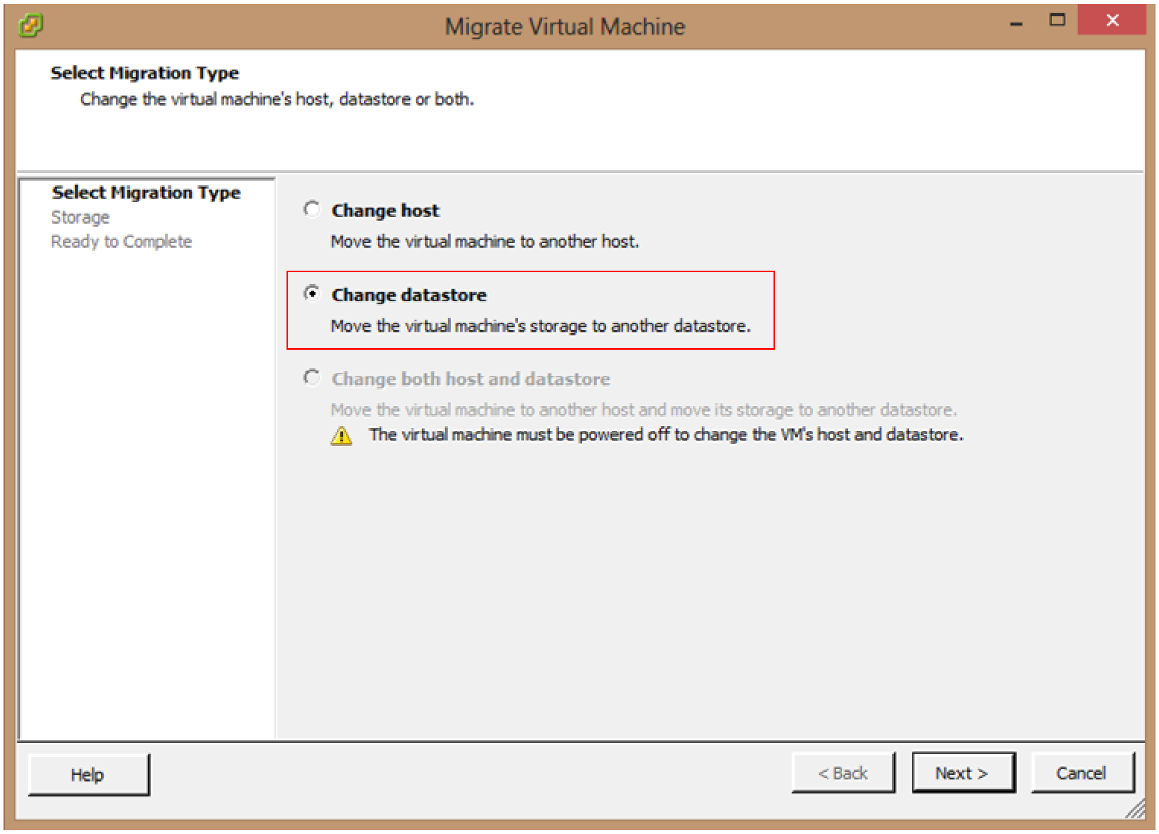
6. Click **Boot VM**:


LiveBoot™ Progress
✓ Gathering information
✓ Logging into ESXi server
✓ Setting data center
✓ Setting hostname
✓ Setting datastore
✓ Enabling VNC
✓ Starting Virtual Machine
✓ Booting Virtual Machine
BARRACUDA NETWORKS
Download vSphere to control VM
Launch VNC to control VM
Dismiss

7. Once the process is complete, log in to vCenter with your vSphere client.
8. Right-click on the LiveBooted virtual machine, and click **Migrate**:


vcenter.largestuff.local
Ann Arbor
vmotion
[redacted]
[redacted]
Ann Arbor Dev
[redacted]
[redacted]
Ann Arbor SE
[redacted]
SE-Ub
SQL20
SQL20
SQL20
WS20
WS20
WS20
WS2K
WS2K
WS2K
WS2K
WS2K
WS2K
Power
Guest
Snapshot
Open Console
Edit Settings...
Migrate...
Clone...
Template
Fault Tolerance
VM Storage Profile
Add Permission... Ctrl+P
Alarm
Report Performance...
Rename
Open in New Window... Ctrl+Alt+N
Remove from Inventory
Delete from Disk

9. In the **Migrate Virtual Machine** page, select **Change datastore**:


Migrate Virtual Machine
Select Migration Type
Storage
Ready to Complete
Help
< Back
Next >
Cancel

Select Migration Type

Change the virtual machine's host, datastore or both.

○ **Change host**

Move the virtual machine to another host.

● **Change datastore**

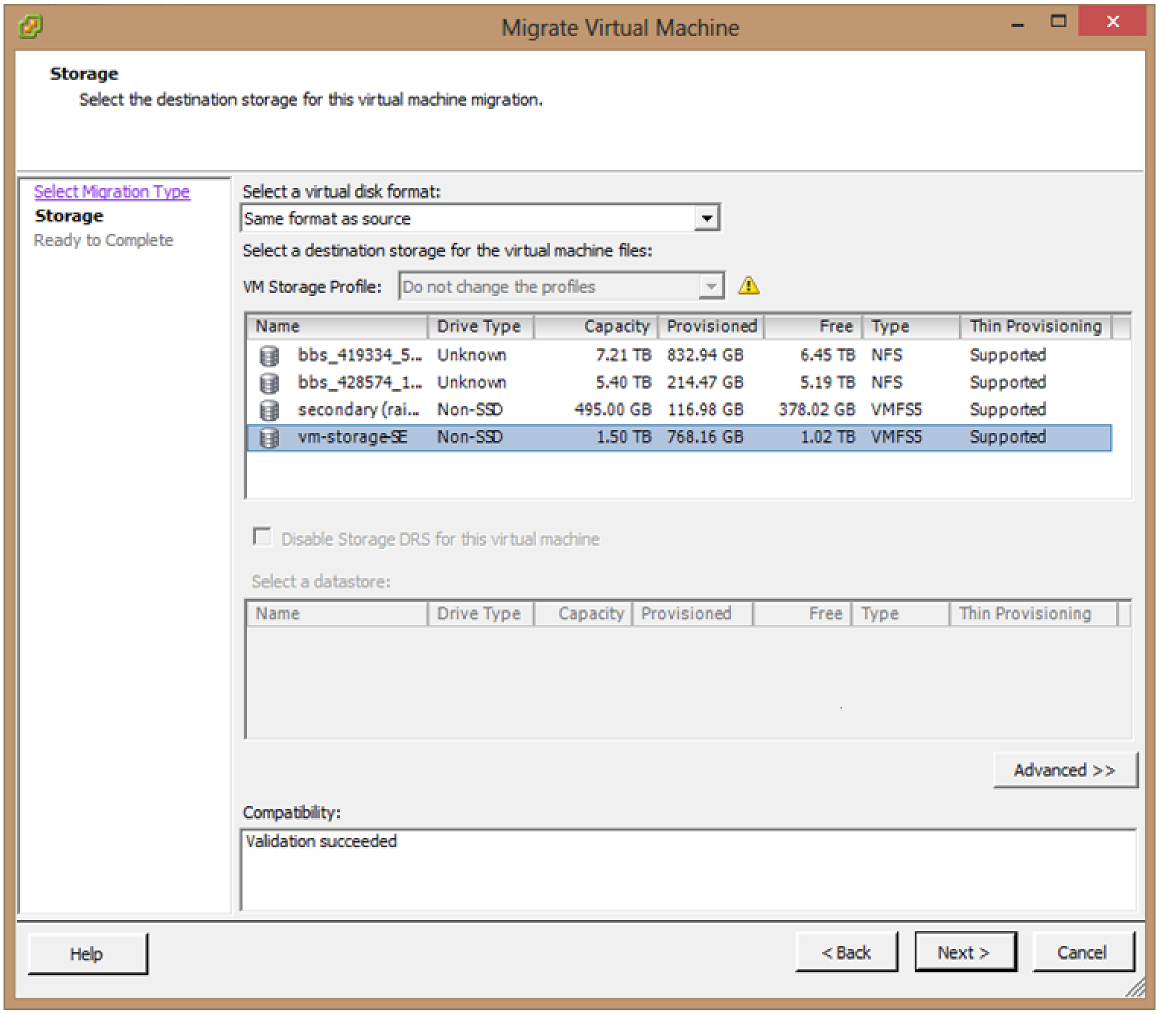
Move the virtual machine's storage to another datastore.

○ **Change both host and datastore**

Move the virtual machine to another host and move its storage to another datastore.

⚠ The virtual machine must be powered off to change the VM's host and datastore.

10. Click **Next**. In the **Storage** page, select the destination storage:



Storage

Select the destination storage for this virtual machine migration.

Select a virtual disk format: Same format as source

Select a destination storage for the virtual machine files:

VM Storage Profile: Do not change the profiles

Name	Drive Type	Capacity	Provisioned	Free	Type	Thin Provisioning
bbs_419334_5...	Unknown	7.21 TB	832.94 GB	6.45 TB	NFS	Supported
bbs_428574_1...	Unknown	5.40 TB	214.47 GB	5.19 TB	NFS	Supported
secondary (rai...	Non-SSD	495.00 GB	116.98 GB	378.02 GB	VMFS5	Supported
vm-storage-SE	Non-SSD	1.50 TB	768.16 GB	1.02 TB	VMFS5	Supported

☐ Disable Storage DRS for this virtual machine

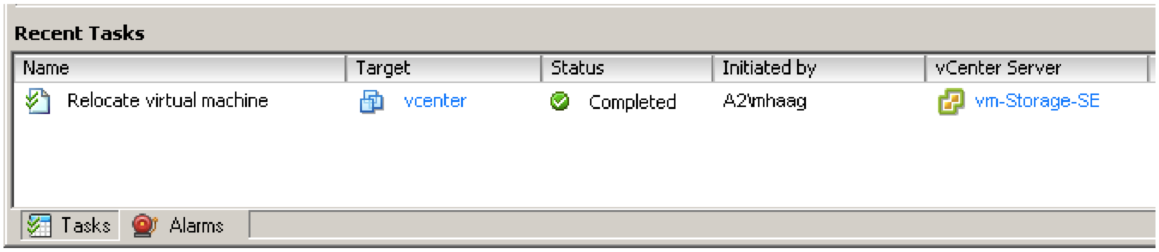
Select a datastore:

Name	Drive Type	Capacity	Provisioned	Free	Type	Thin Provisioning

Compatibility:

Validation succeeded

11. Click **Next**, and then click **Finish** in the **Ready to Complete** page.
12. In vCenter, the **Relocate virtual machine** task displays under **Recent Tasks**, and the status displays as **Completed**:



Recent Tasks

Name	Target	Status	Initiated by	vCenter Server
Relocate virtual machine	vcenter	Completed	A2\mhaag	vm-Storage-SE

Barracuda copy.com

In this Section

- How to Restore to a copy.com Account
- How to Share and View Files Using copy.com

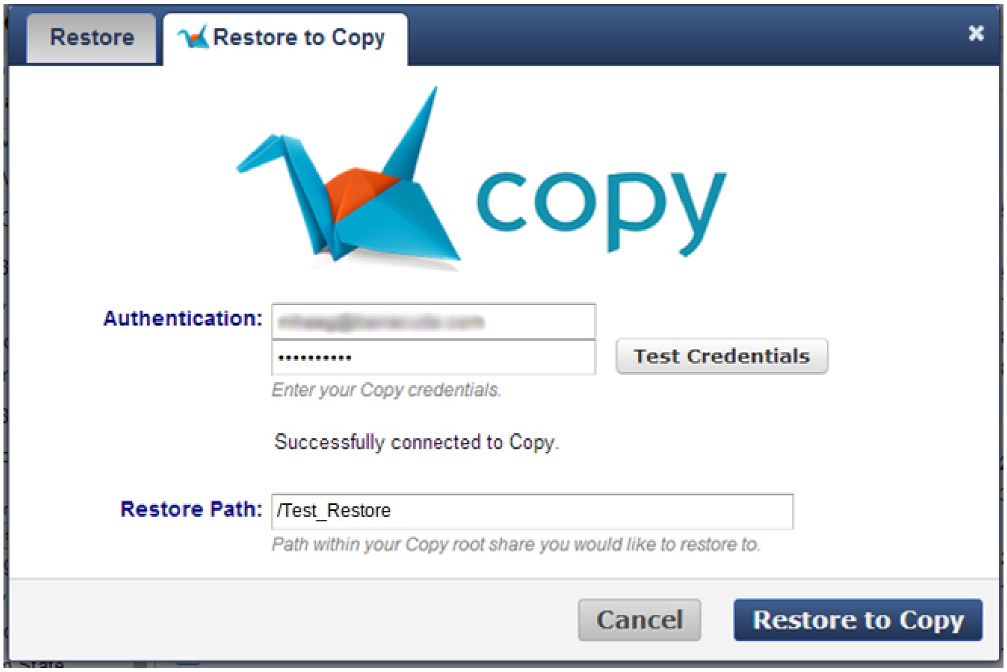
How to Restore to a copy.com Account

This article refers to Barracuda Backup firmware version 5.1 and higher, and both privately and publicly shared **copy.com** accounts . This feature is available only if your copy.com account has cloud subscriptions and data is replicated to the cloud.

Related Articles
- How to Share and View Files Using copy.com

Use the following steps to restore your copy.com account,

1. Log in to the Barracuda Backup web interface, and click **RESTORE**.
2. In the **Restore Browser** pane, navigate to and select the Copy content you want to restore.
3. In the right pane, drill into the content and select the file or folder for restore, and click **Restore**.
4. The **Restore** dialog displays.
5. Click the **Restore to Copy** tab, and enter your username and password in the associated fields.
6. Click **Test Credentials** to verify your Copy credentials.
7. In the **Restore Path** field, enter the path within your Copy root share where you want to restore the files:



Authentication: ••••••••••

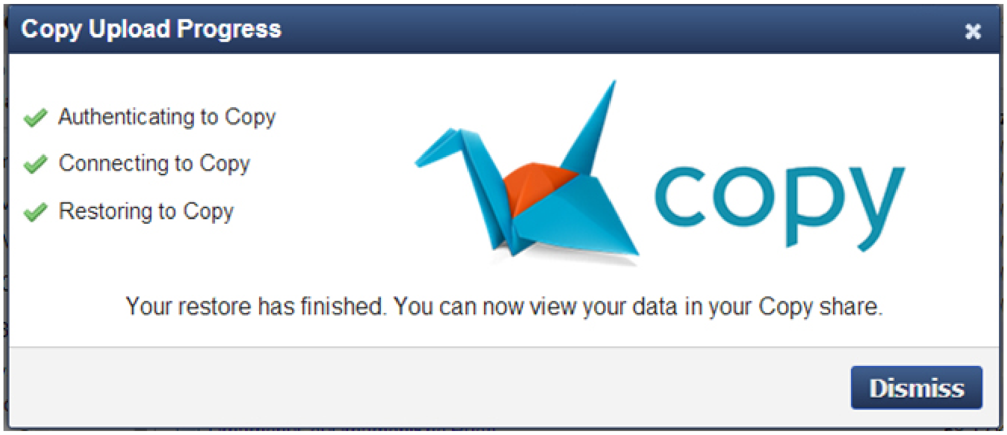
Enter your Copy credentials.

Successfully connected to Copy.

Restore Path: /Test_Restore

Path within your Copy root share you would like to restore to.

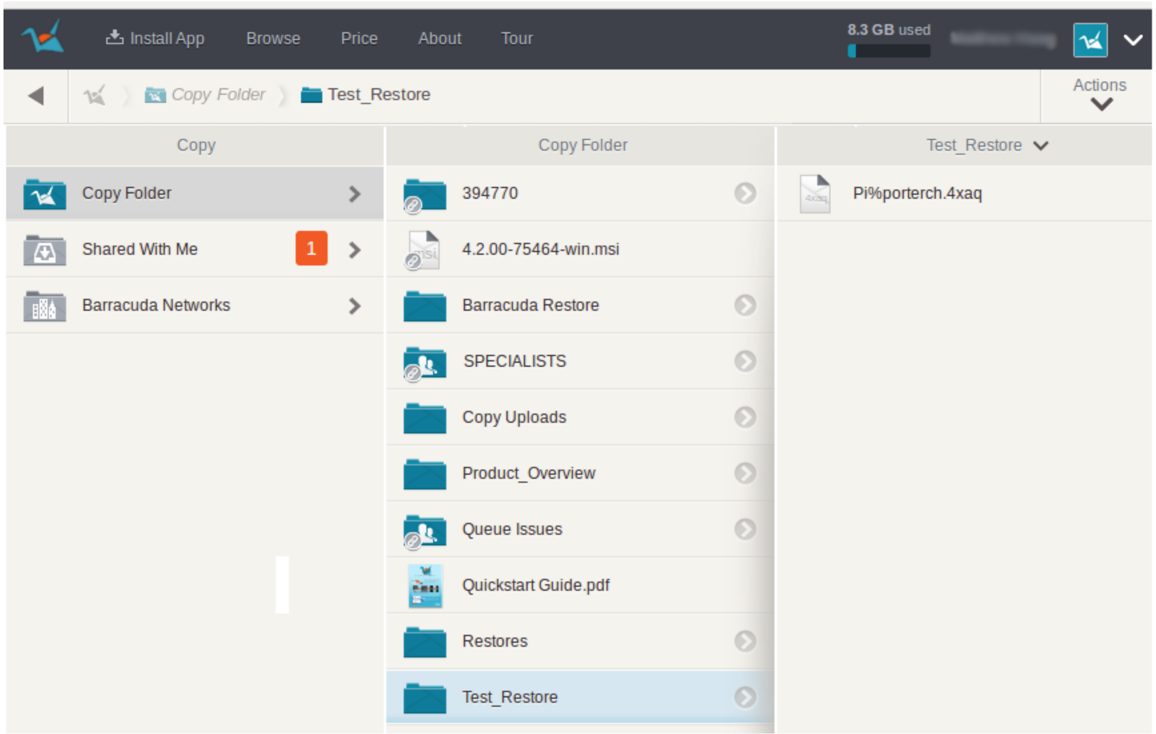
8. Click **Restore to Copy**.
9. The **Copy Upload Progress** dialog displays:



✓ Authenticating to Copy
✓ Connecting to Copy
✓ Restoring to Copy

Your restore has finished. You can now view your data in your Copy share.

10. The upload is complete once a check mark (✓) displays in front of each action.
11. Click **Dismiss** to close the dialog. The restore is complete.
12. Log into Copy to view the restored content:


Install App
Browse
Price
About
Tour
8.3 GB used
Copy Folder
Test_Restore
Actions
Copy
Copy Folder
Test_Restore
Copy Folder
Shared With Me
1
Barracuda Networks
394770
4.2.00-75464-win.msi
Barracuda Restore
SPECIALISTS
Copy Uploads
Product_Overview
Queue Issues
Quickstart Guide.pdf
Restores
Test_Restore
Pi%porterch.4xaq

How to Share and View Files Using copy.com

This article refers to Barracuda Backup firmware version 5.1 and higher.

In this article:

- Share Files
- View Files

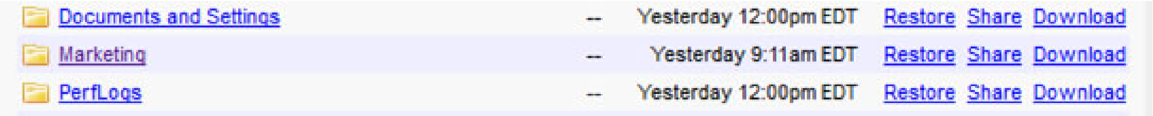
Related Articles

- How to Restore to a copy.com Account

Share Files

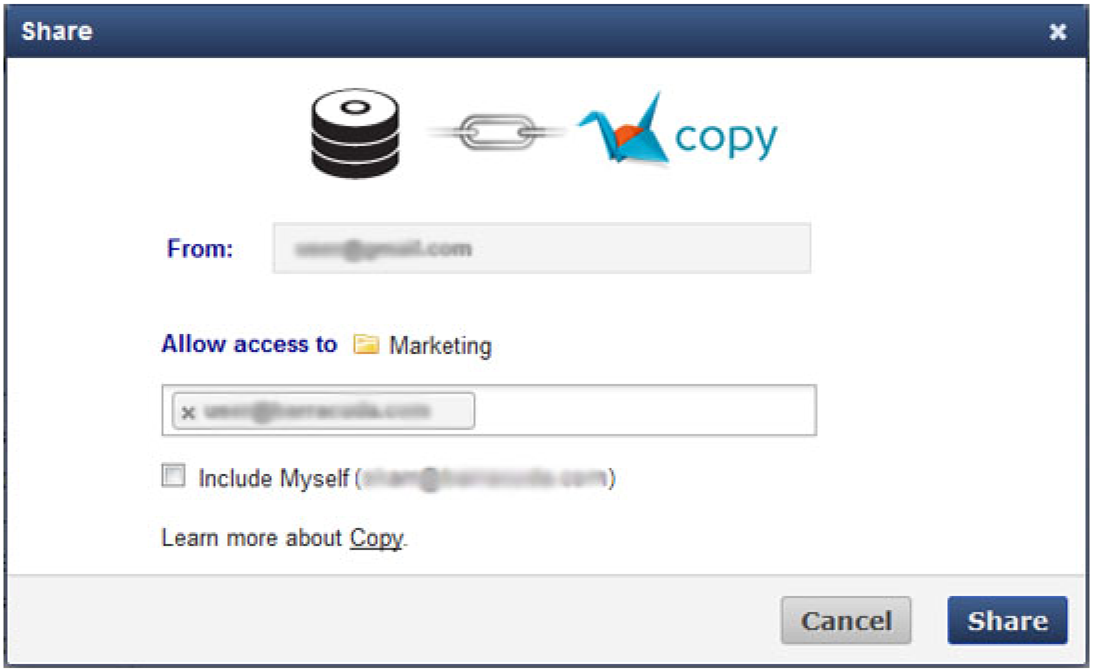
Use copy.com to easily share files and directories with remote or traveling employees. Use the following steps to share files using copy.com:

1. Log in to login.barracuda.com, and select the associated Barracuda Backup Server in the left pane.
2. Click **Restore**, navigate to the file or directory you want to share, and click **Share**:



Documents and Settings	--	Yesterday 12:00pm EDT	Restore	Share	Download
Marketing	--	Yesterday 9:11am EDT	Restore	Share	Download
PerfLogs	--	Yesterday 12:00pm EDT	Restore	Share	Download

3. The selected folder displays in the **Allow access to** field.
4. Enter your copy.com credentials, and add the email address of the user(s) with whom to share the selected content:



From: [redacted]

Allow access to Marketing

× [redacted]

☐ Include Myself ([redacted])

Learn more about Copy.

5. Click **Share**, and then click **OK**.
6. An email is sent to the specified user(s) with a link to the shared data on copy.com.

View Files

To view the shared file or directory:

1. Log in to copy.com. A folder titled __**Devices** displays in your **Copy Folder**.
2. Click through the folder path to view your shared file or directory.

Restore Browser

In this Section

- Understanding Restore Browser
- How to Search for Items Using the Restore Browser
- How to Restore Data Using the Restore Browser

Understanding Restore Browser

Use the Barracuda Backup web interface to restore data that was stored either using the Barracuda Backup Agent or file share data, or to download a file, a file system directory, an email mailbox, or mailbox folders.

This is the recommended way to restore data backed up by the Barracuda Backup Agent. You should know:

- Message-level data must be restored to the computer from which it originally came
- Data can be restored back to its original location or to another computer on your network. If restoring to another location, the Barracuda Backup Agent must be installed on that system
- A functioning Barracuda Backup Server must be in place in order to restore SQL Server and Microsoft® Exchange databases

File Share Data

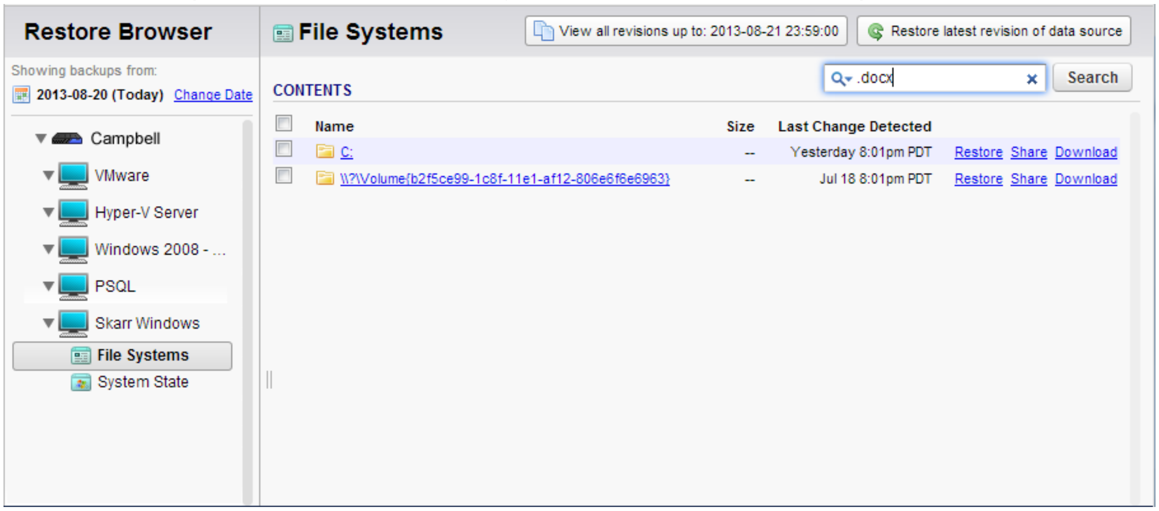
When restoring file share data through the web interface, you can restore one file at a time, a single directory, or an entire share. This works well when you only need to restore a few documents. File share data can be restored to its original location through the web interface.

How to Search for Items Using the Restore Browser

This article applies to Barracuda Backup Server firmware version 5.3.00 and higher.

Use the following steps to search for items using the restore browser:

1. Log in to the Barracuda Backup web interface using https://login.barracudanetworks.com/, and select the associated Barracuda Backup Server in the left pane.
2. Go to the **RESTORE > Restore Browser** page, and select the target data source.
3. Enter a word or phrase as the search string in the **Search** field, for example, enter the file extension **.docx**:

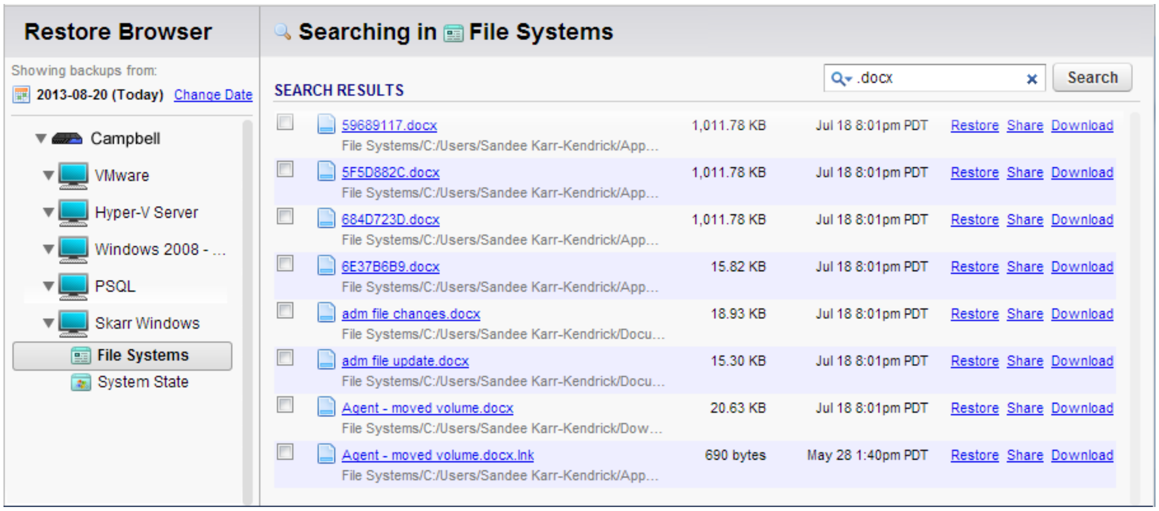

Restore Browser
Showing backups from:
2013-08-20 (Today)
Change Date
Campbell
VMware
Hyper-V Server
Windows 2008 - ...
PSQL
Skarr Windows
File Systems
System State
File Systems
View all revisions up to: 2013-08-21 23:59:00
Restore latest revision of data source
Search

Search field: .docx

CONTENTS

☐	Name	Size	Last Change Detected			
☐	C:	--	Yesterday 8:01pm PDT	Restore	Share	Download
☐	\\?\Volume{b2f5ce99-1c8f-11e1-af12-806e6f6e6963}	--	Jul 18 8:01pm PDT	Restore	Share	Download

4. Click **Search**; the search results returns:

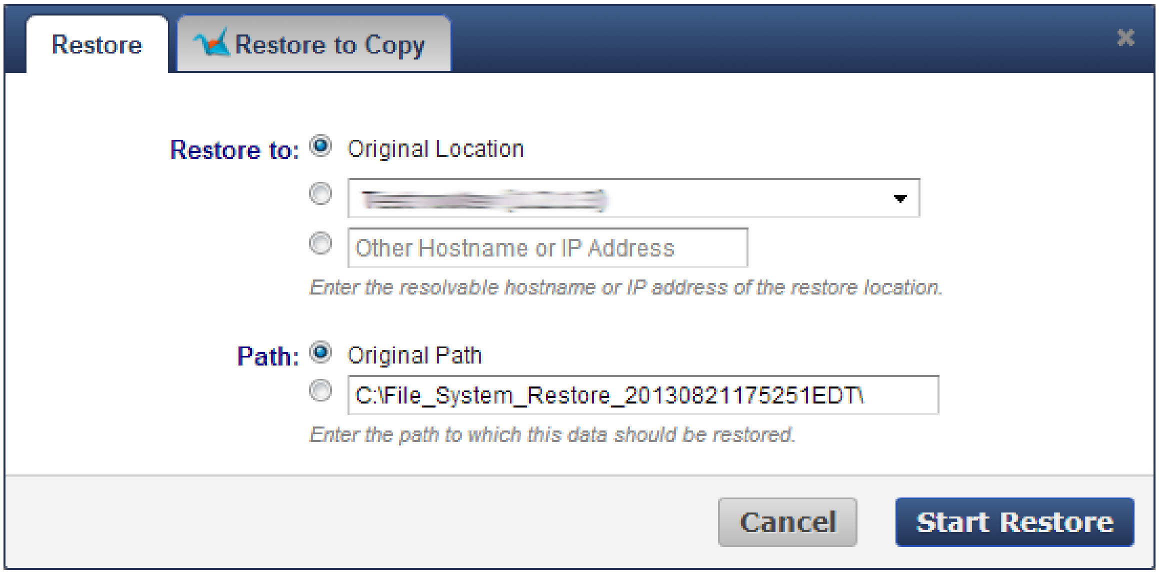

Restore Browser
Showing backups from:
2013-08-20 (Today)
Change Date
Campbell
VMware
Hyper-V Server
Windows 2008 - ...
PSQL
Skarr Windows
File Systems
System State
Searching in File Systems
Search

Search field: .docx

SEARCH RESULTS

☐	59689117.docx File Systems/C:/Users/Sandee Karr-Kendrick/App...	1,011.78 KB	Jul 18 8:01pm PDT	Restore	Share	Download
☐	5F5D882C.docx File Systems/C:/Users/Sandee Karr-Kendrick/App...	1,011.78 KB	Jul 18 8:01pm PDT	Restore	Share	Download
☐	684D723D.docx File Systems/C:/Users/Sandee Karr-Kendrick/App...	1,011.78 KB	Jul 18 8:01pm PDT	Restore	Share	Download
☐	6E37B6B9.docx File Systems/C:/Users/Sandee Karr-Kendrick/App...	15.82 KB	Jul 18 8:01pm PDT	Restore	Share	Download
☐	adm file changes.docx File Systems/C:/Users/Sandee Karr-Kendrick/Docu...	18.93 KB	Jul 18 8:01pm PDT	Restore	Share	Download
☐	adm file update.docx File Systems/C:/Users/Sandee Karr-Kendrick/Docu...	15.30 KB	Jul 18 8:01pm PDT	Restore	Share	Download
☐	Agent - moved volume.docx File Systems/C:/Users/Sandee Karr-Kendrick/Dow...	20.63 KB	Jul 18 8:01pm PDT	Restore	Share	Download
☐	Agent - moved volume.docx.lnk File Systems/C:/Users/Sandee Karr-Kendrick/App...	690 bytes	May 28 1:40pm PDT	Restore	Share	Download

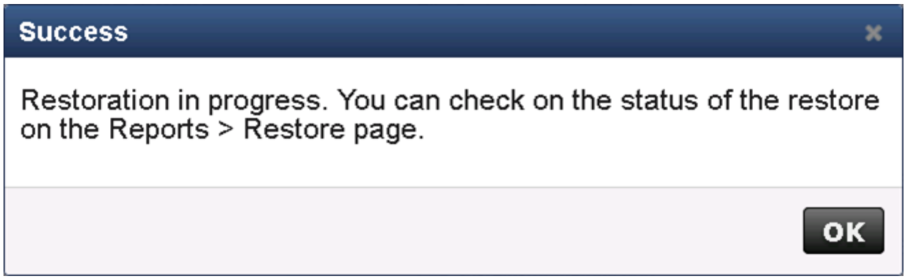
5. Identify the item you wish to restore, and click **Restore**; the **Restore** dialog box displays:



Restore to: ● Original Location
○ [redacted]
○ Other Hostname or IP Address
Enter the resolvable hostname or IP address of the restore location.

Path: ● Original Path
○ C:\File_System_Restore_20130821175251EDT\
Enter the path to which this data should be restored.

6. In the **Restore** tab, select the **Restore to** location and **Path**, and then click **Start Restore**.
7. Once the restore is complete, the **Success** dialog displays:



Restoration in progress. You can check on the status of the restore on the Reports > Restore page.

8. Restore details are available on the **REPORTS > Restore** page.

How to Restore Data Using the Restore Browser

Use the Barracuda Backup web interface to restore data that was stored either using the Barracuda Backup Agent or file share data, or to download a file, a file system directory, an email mailbox, or mailbox folders.

In this article:

- Requirements
- File Share Data
- Backup Data by Date
- Restore Data
- Restore a Revision
- Restore Latest Revision
- Download Files and Directories

This is the recommended way to restore data backed up by the Barracuda Backup Agent. You should know:

- Message-level data must be restored to the computer from which it originally came
- Data can be restored back to its original location or to another computer on your network. If restoring to another location, the Barracuda Backup Agent must be installed on that system
- A functioning Barracuda Backup Server must be in place in order to restore SQL Server and Microsoft® Exchange databases

Requirements

When restoring data backed up by the Barracuda Backup Agent:

- Message-level data must be restored to the computer from which it originally came.

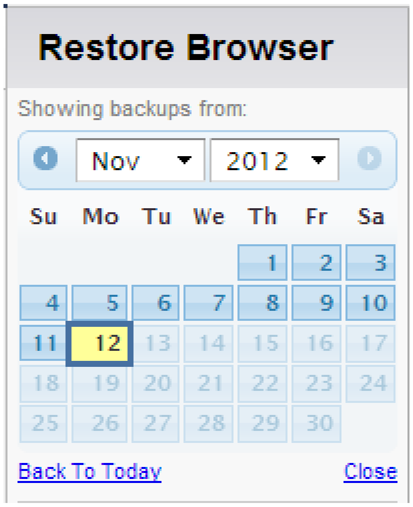
- Data can be restored back to its original location, or to another computer on your network. If restoring to another location, the Barracuda Backup Agent must be installed on that system.
- A functioning Barracuda Backup Server must be in place in order to restore a SQL Server and Microsoft® Exchange databases.

File Share Data

When restoring file share data through the web interface, you can restore one file at a time, a single directory, or an entire share. This works well when you only need to restore a few documents. File share data can be restored to its original location through the web interface, or for Barracuda Backup firmware release 4.3 and earlier, you can use Barracuda Restore for Windows to restore file share data to its original location.

Backup Data by Date

By default, the **Restore Browser** page displays backups as of the current date. To select backups from an earlier date, click **Change Date** in the left pane, and select the desired date:



Click **Close** to hide the date selection view.

Restore Data

1. Select the Barracuda Backup Server from which to restore data, and go to the **RESTORE > Restore Browser** page.
2. In the left pane, select the computer and the associated data source that contains the files you want to restore.
3. In the right pane, navigate to and click on the content you want to restore, and click **Restore**.
4. In the **Restore** dialog, select a local location where you want to restore the data, or enter a resolvable hostname or IP address of a restore location.
5. Select the **Original Path**, or enter a new path to which to restore the data, and click **Start Restoring**.
6. Go to the **REPORTS > Restore** page to view the restore status; click on a report to view individually restored items.
7. To stop the restoration process, go to the **REPORTS > Restore** page, and click **Abort Restore**.

Restore a Revision

For file systems and system state, you can select a revision to which to restore.

1. Select the Barracuda Backup Server from which to restore data, and go to the **RESTORE > Restore Browser** page.
2. In the left pane, select the computer and the associated data source that contains the files you want to restore.
3. In the right pane, click **View all revisions up to *[date]***; all available revisions display.
4. Click **Restore** following the revision you want to restore.

Restore Latest Revision

1. Select the Barracuda Backup Server from which to restore data, and go to the **RESTORE > Restore Browser** page.
2. In the left pane, select the computer and the associated data source that contains the files you want to restore.
3. In the right pane, click **Restore Latest Revision of Data Source**. The **Restore Latest Revision of Data Source** dialog box displays.
4. Select whether to restore to the original location, select an alternate location from the drop-down menu, or enter a resolvable hostname or IP address of the restore location.
5. click **Start Restore**.

Download Files and Directories

You can select to download files and directories directly to your system. Click **Download** in the right pane to:

- Download a single file
- Download file system directories as ZIP files
- Download email mailboxes and folders as ZIP files

How to Restore from Local and Offsite Backups

Data can be restored from the local Barracuda Backup Server, from a remote Barracuda Backup Server that has been used to replicate that system, or from the Barracuda Cloud Storage. Restores from the local Barracuda Backup Server offer the fastest restore times.

In this article:

- Restore Methods
- Restore Data Backed Up by the Barracuda Backup Agent
- Restore File Share Data

Related Articles
• Restore by Overwriting Existing Database • Restore Using a Recovery Storage Group • VMware Server Recovery and Restoration • Restore Exchange and GroupWise Messages

Restore Methods

Multiple methods are available to restore your backed-up data including:

- Restore Browser in the Barracuda Backup web interface
- Barracuda Restore for Windows
- Restore from a Replication Destination
- How to Restore Data with FTPES

You can restore single files, individual email messages, and entire systems.

Restore Data Backed Up by the Barracuda Backup Agent

Data backed up by the Barracuda Backup Agent can be restored using the following methods:

- Restore Browser in the Barracuda Backup Server web interface (recommended)
- Barracuda Restore for Windows (firmware release 4.3 and earlier)

Restore File Share Data

File share data can be restored using any of the following methods:

- Barracuda Restore for Windows (firmware release 4.3 and earlier)
- Restore Browser in the Barracuda Backup web interface
- FTP from Barracuda Backup Server
- How to Restore Data with FTPES

How to Recover Backed Up Data

This article refers to Barracuda Backup firmware version 5.0 or higher.

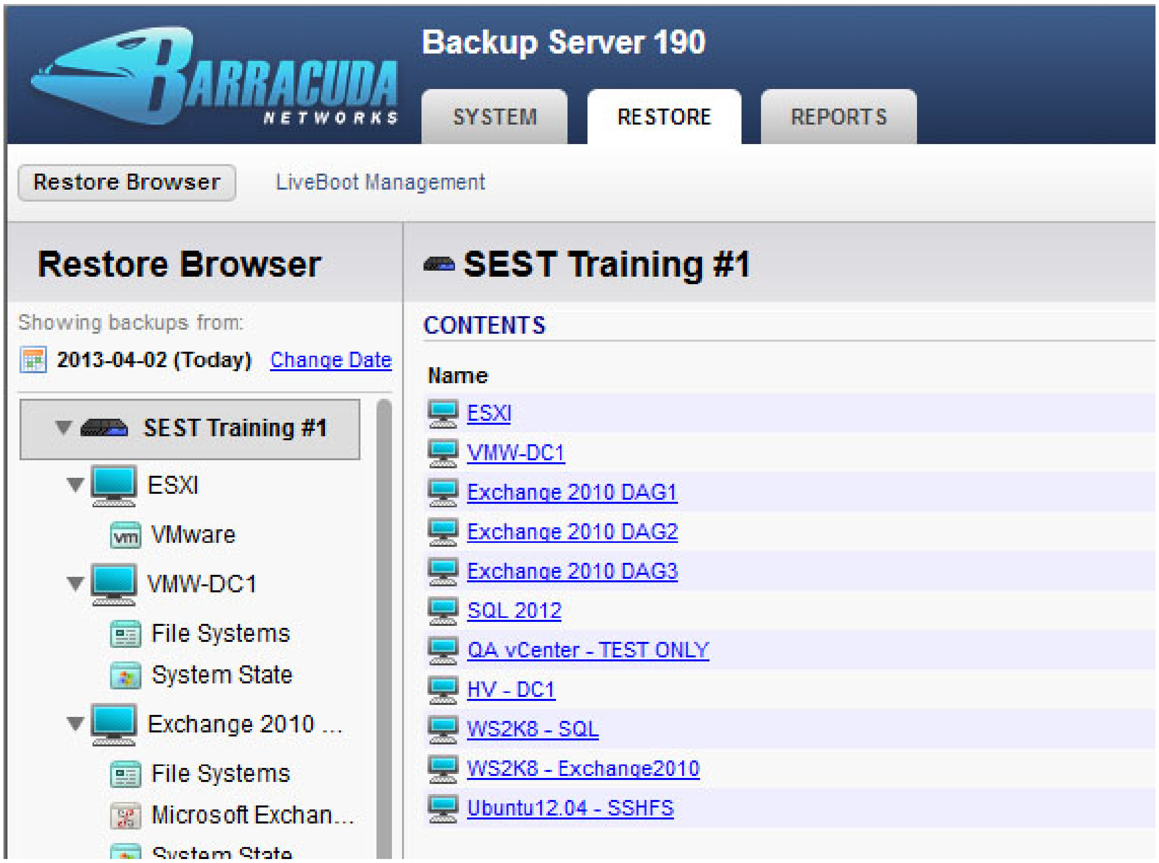
You can recover backed up content either from the local web interface or from the cloud.

- **Local Device Web Interface** - To download from the local device at LAN speeds, use the Download feature in the Barracuda Backup local web interface.
- **Cloud Web Interface** - To verify and download data from the cloud, use the hosted Barracuda Backup web interface login credentials.

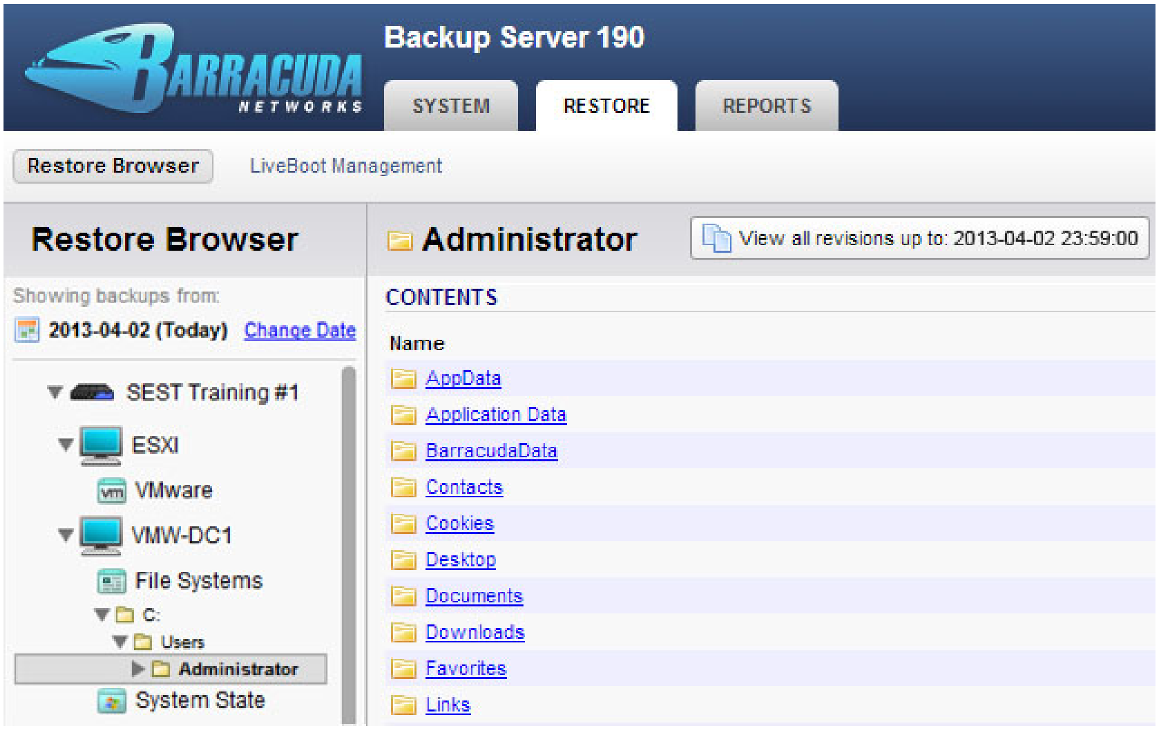
Download Using the Local Device Web Interface

Use the Barracuda Backup Download feature through the local web interface to quickly download backed up data. The following steps describe how to use this feature:

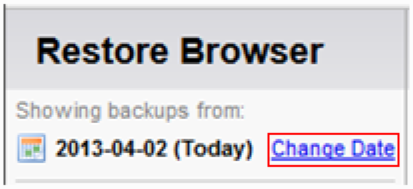
1. Open a web browser, enter the Barracuda Backup Server IP address, and log in to the Barracuda Backup web interface.
2. The **System** page displays; go to the **RESTORE > Restore Browser** page:


BARRACUDA NETWORKS
Backup Server 190
SYSTEM
RESTORE
REPORTS
Restore Browser
LiveBoot Management
Restore Browser
SEST Training #1
Showing backups from:
2013-04-02 (Today)
Change Date
SEST Training #1
ESXI
VMware
VMW-DC1
File Systems
System State
Exchange 2010 ...
File Systems
Microsoft Exchan...
System State
CONTENTS
Name
ESXI
VMW-DC1
Exchange 2010 DAG1
Exchange 2010 DAG2
Exchange 2010 DAG3
SQL 2012
QA vCenter - TEST ONLY
HV - DC1
WS2K8 - SQL
WS2K8 - Exchange2010
Ubuntu12.04 - SSHFS

3. Navigate to a directory or file for download:

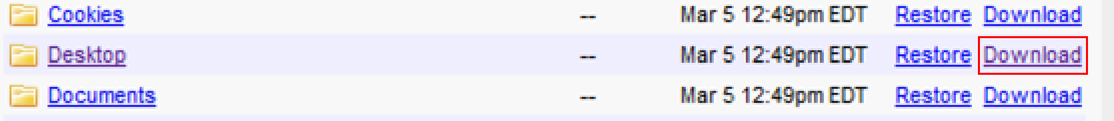

Backup Server 190
BARRACUDA NETWORKS
SYSTEM
RESTORE
REPORTS
Restore Browser
LiveBoot Management
Restore Browser
Showing backups from:
2013-04-02 (Today)
Change Date
SEST Training #1
ESXI
VMware
VMW-DC1
File Systems
C:
Users
Administrator
System State
Administrator
View all revisions up to: 2013-04-02 23:59:00
CONTENTS
Name
AppData
Application Data
BarracudaData
Contacts
Cookies
Desktop
Documents
Downloads
Favorites
Links

4. The **Restore Browser** section displays the latest backup date.

> **Older Revision**
> To restore an older revision of the file or directory, click **Change Date** to display all available revisions:
>
> 
>

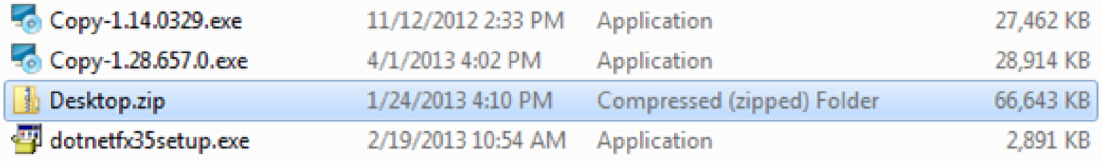
Restore Browser
> Showing backups from:
> 2013-04-02 (Today)
> Change Date

5. Click **Download** to the right of the file or folder you want to download:



Cookies	--	Mar 5 12:49pm EDT	Restore	Download
Desktop	--	Mar 5 12:49pm EDT	Restore	Download
Documents	--	Mar 5 12:49pm EDT	Restore	Download

6. The selected file is downloaded to a zip file. Once downloaded, you can extract the downloaded content from the zip file:

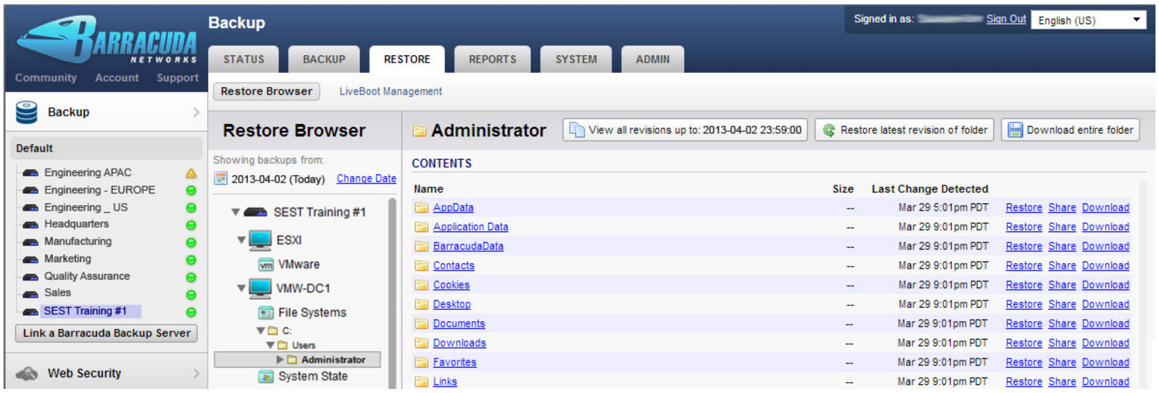


Copy-1.14.0329.exe	11/12/2012 2:33 PM	Application	27,462 KB
Copy-1.28.657.0.exe	4/1/2013 4:02 PM	Application	28,914 KB
Desktop.zip	1/24/2013 4:10 PM	Compressed (zipped) Folder	66,643 KB
dotnetfx35setup.exe	2/19/2013 10:54 AM	Application	2,891 KB

Download Using the Cloud Web Interface

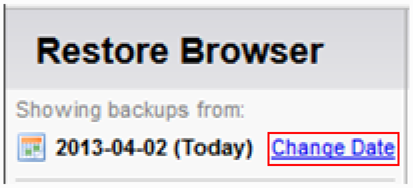
Use the following steps to download and verify backed up data from the cloud:

1. Go to https://login.barracudanetworks.com/ and log in to the Barracuda Backup web interface.
2. Go to the **RESTORE > Restore Browser** page.
3. Navigate to a file or folder for download:


Backup
STATUS
BACKUP
RESTORE
REPORTS
SYSTEM
ADMIN
Signed in as: [redacted] Sign Out
English (US)
Community
Account
Support
Restore Browser
LiveBoot Management
Backup
Default
Engineering APAC
Engineering - EUROPE
Engineering _ US
Headquarters
Manufacturing
Marketing
Quality Assurance
Sales
SEST Training #1
Link a Barracuda Backup Server
Web Security
Restore Browser
Showing backups from:
2013-04-02 (Today) Change Date
SEST Training #1
ESXI
VMware
VMW-DC1
File Systems
C:
Users
Administrator
System State
Administrator
View all revisions up to: 2013-04-02 23:59:00
Restore latest revision of folder
Download entire folder
CONTENTS

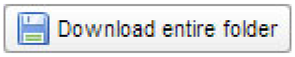
Name	Size	Last Change Detected			
AppData	--	Mar 29 5:01pm PDT	Restore	Share	Download
Application Data	--	Mar 29 9:01pm PDT	Restore	Share	Download
BarracudaData	--	Mar 29 9:01pm PDT	Restore	Share	Download
Contacts	--	Mar 29 9:01pm PDT	Restore	Share	Download
Cookies	--	Mar 29 9:01pm PDT	Restore	Share	Download
Desktop	--	Mar 29 9:01pm PDT	Restore	Share	Download
Documents	--	Mar 29 9:01pm PDT	Restore	Share	Download
Downloads	--	Mar 29 9:01pm PDT	Restore	Share	Download
Favorites	--	Mar 29 9:01pm PDT	Restore	Share	Download
Links	--	Mar 29 9:01pm PDT	Restore	Share	Download

4. The Restore Browser section displays the latest backup date.

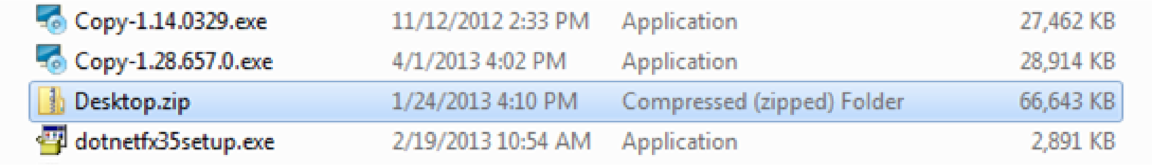
> **Older Revision**
> To restore an older revision of the file or directory, click **Change Date** to display all available revisions:
>
> 
>

Restore Browser
> Showing backups from:
> 2013-04-02 (Today)
> Change Date

5. Click **Download** to the right of the file or folder you want to download, or click **Download entire folder** to download all content within the folder selected in the **Restore Browser** section:


Download entire folder

6. The content is downloaded as a .zip file. Once downloaded, you can extract the downloaded content from the zip file:



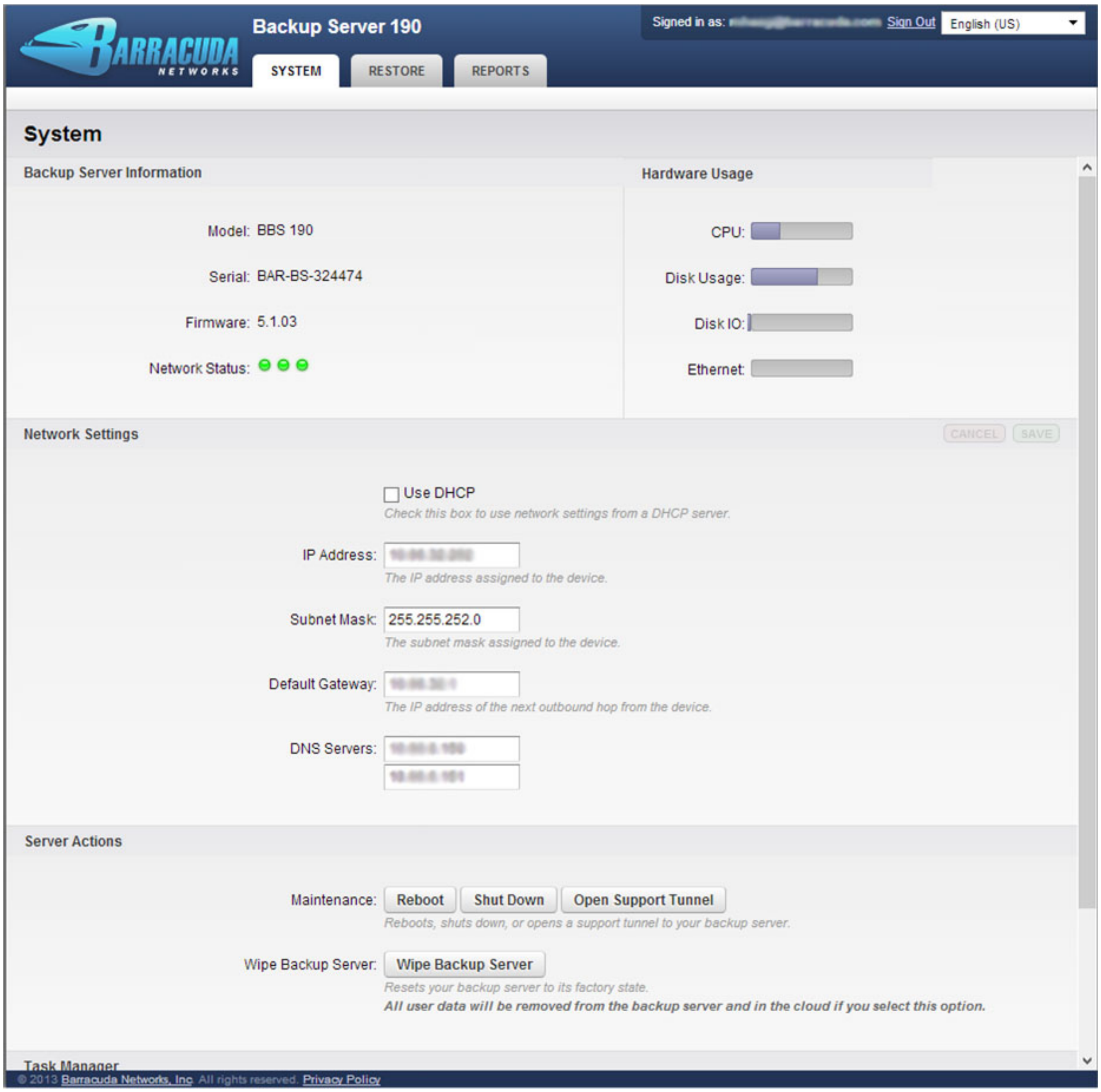
Copy-1.14.0329.exe	11/12/2012 2:33 PM	Application	27,462 KB
Copy-1.28.657.0.exe	4/1/2013 4:02 PM	Application	28,914 KB
Desktop.zip	1/24/2013 4:10 PM	Compressed (zipped) Folder	66,643 KB
dotnetfx35setup.exe	2/19/2013 10:54 AM	Application	2,891 KB

Example - Restore Data Using the Local Web Interface

> This article refers to Barracuda Backup firmware 5.1 and higher.

Use the following steps to restore data using the Barracuda Backup local web interface. Note that the local web interface does not require an Internet connection which may improve performance.

1. Open a web browser, and enter the Barracuda Backup Server IP address.
2. Log into the Barracuda Backup web interface; the **System** page displays:


Backup Server 190
Signed in as: [redacted] Sign Out
English (US)
SYSTEM
RESTORE
REPORTS
CANCEL
SAVE
Reboot
Shut Down
Open Support Tunnel
Wipe Backup Server
Task Manager
© 2013 Barracuda Networks, Inc. All rights reserved. Privacy Policy

System

Backup Server Information

Model: BBS 190
Serial: BAR-BS-324474
Firmware: 5.1.03
Network Status: ● ● ●

Hardware Usage

CPU:
Disk Usage:
Disk IO:
Ethernet:

Network Settings

☐ Use DHCP
Check this box to use network settings from a DHCP server.

IP Address: [redacted]
The IP address assigned to the device.

Subnet Mask: 255.255.252.0
The subnet mask assigned to the device.

Default Gateway: [redacted]
The IP address of the next outbound hop from the device.

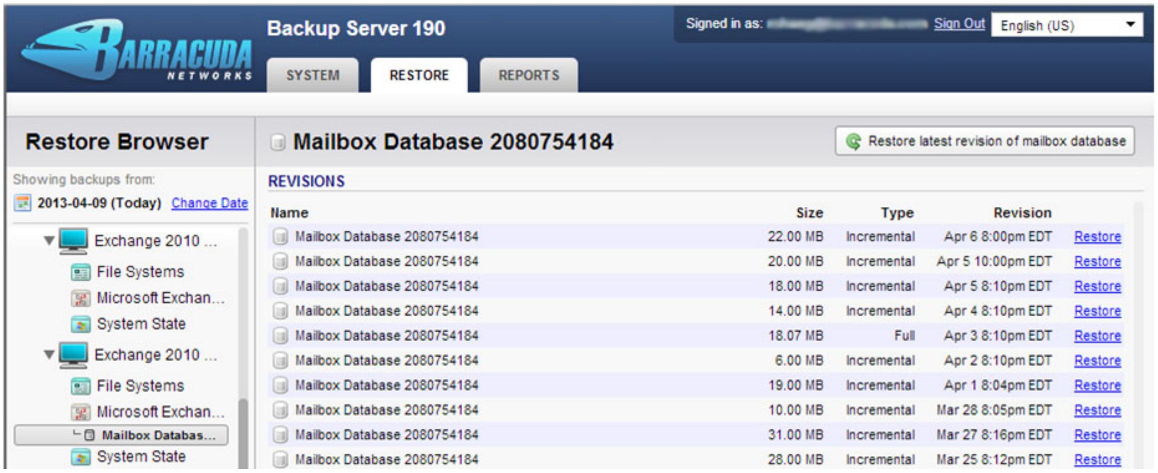
DNS Servers: [redacted]

Server Actions

Maintenance: Reboot | Shut Down | Open Support Tunnel
Reboots, shuts down, or opens a support tunnel to your backup server.

Wipe Backup Server: Wipe Backup Server
Resets your backup server to its factory state.
All user data will be removed from the backup server and in the cloud if you select this option.

3. Click the **RESTORE** tab, and select the server from which to restore data. In the following example, a Microsoft Exchange Database is selected:


Backup Server 190
Signed in as: [redacted] Sign Out
English (US)
SYSTEM
RESTORE
REPORTS
Restore latest revision of mailbox database
Exchange 2010 ...
File Systems
Microsoft Exchan...
System State
Exchange 2010 ...
File Systems
Microsoft Exchan...
Mailbox Databas...
System State

Restore Browser

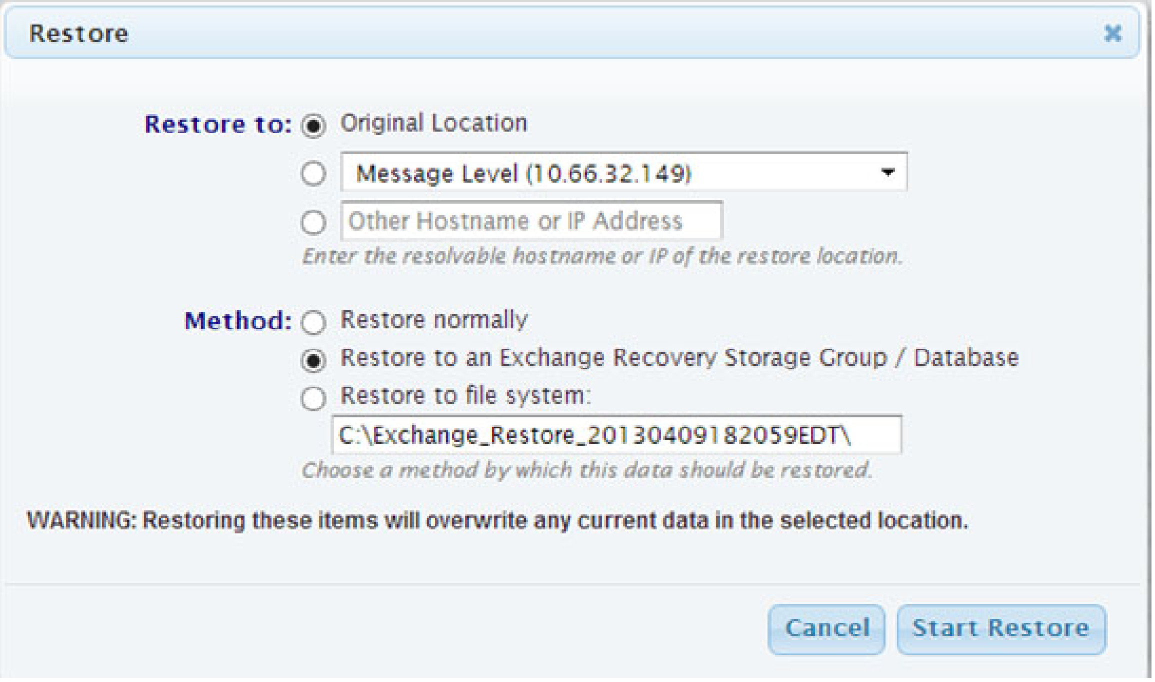
Showing backups from:
2013-04-09 (Today) Change Date

Mailbox Database 2080754184

REVISIONS

Name	Size	Type	Revision	
Mailbox Database 2080754184	22.00 MB	Incremental	Apr 6 8:00pm EDT	Restore
Mailbox Database 2080754184	20.00 MB	Incremental	Apr 5 10:00pm EDT	Restore
Mailbox Database 2080754184	18.00 MB	Incremental	Apr 5 8:10pm EDT	Restore
Mailbox Database 2080754184	14.00 MB	Incremental	Apr 4 8:10pm EDT	Restore
Mailbox Database 2080754184	18.07 MB	Full	Apr 3 8:10pm EDT	Restore
Mailbox Database 2080754184	6.00 MB	Incremental	Apr 2 8:10pm EDT	Restore
Mailbox Database 2080754184	19.00 MB	Incremental	Apr 1 8:04pm EDT	Restore
Mailbox Database 2080754184	10.00 MB	Incremental	Mar 28 8:05pm EDT	Restore
Mailbox Database 2080754184	31.00 MB	Incremental	Mar 27 8:16pm EDT	Restore
Mailbox Database 2080754184	28.00 MB	Incremental	Mar 25 8:12pm EDT	Restore

4. Click the **Restore** link to the right of the data you wish to restore; the **Restore** window displays. Select the **Restore to** and **Method** for restoring the data, for example, select **Original Location** to select the original server, and select **Restore to an Exchange Recovery Storage Group/Database** to restore to a recovery database:



Restore to: ● Original Location

○ Message Level (10.66.32.149)

○ Other Hostname or IP Address

Enter the resolvable hostname or IP of the restore location.

Method: ○ Restore normally

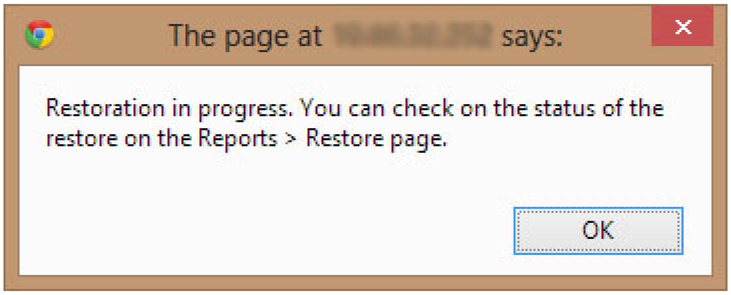
● Restore to an Exchange Recovery Storage Group / Database

○ Restore to file system: C:\Exchange_Restore_20130409182059EDT\

Choose a method by which this data should be restored.

WARNING: Restoring these items will overwrite any current data in the selected location.

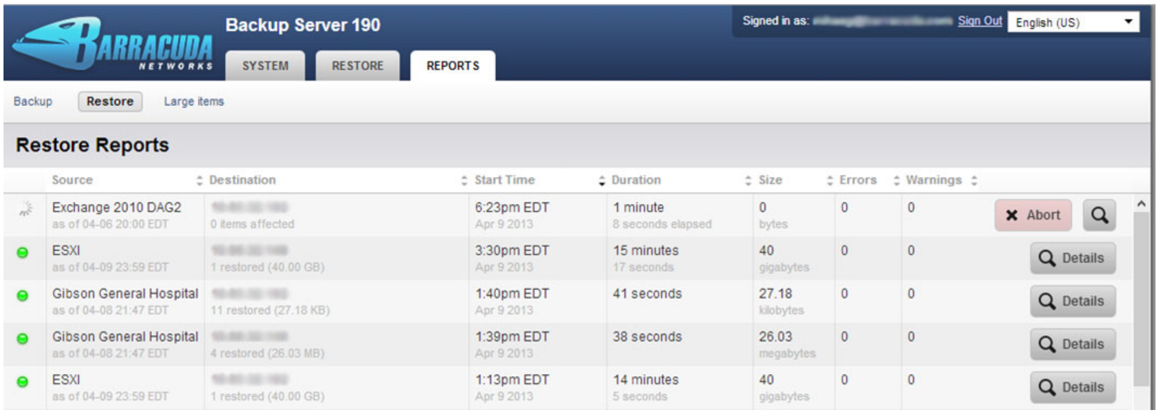
5. Click **Start Restore**; the **Restoration in progress** window displays:



The page at [redacted] says:

Restoration in progress. You can check on the status of the restore on the Reports > Restore page.

6. Click **OK**. In the web interface, go to **REPORTS > Restore** to view the restoration status:



Restore Reports

	Source	Destination	Start Time	Duration	Size	Errors	Warnings	
	Exchange 2010 DAG2 as of 04-06 20:00 EDT	[redacted] 0 items affected	6:23pm EDT Apr 9 2013	1 minute 8 seconds elapsed	0 bytes	0	0	Abort
●	ESXI as of 04-09 23:59 EDT	[redacted] 1 restored (40.00 GB)	3:30pm EDT Apr 9 2013	15 minutes 17 seconds	40 gigabytes	0	0	Details
●	Gibson General Hospital as of 04-08 21:47 EDT	[redacted] 11 restored (27.18 KB)	1:40pm EDT Apr 9 2013	41 seconds	27.18 kilobytes	0	0	Details
●	Gibson General Hospital as of 04-08 21:47 EDT	[redacted] 4 restored (26.03 MB)	1:39pm EDT Apr 9 2013	38 seconds	26.03 megabytes	0	0	Details
●	ESXI as of 04-09 23:59 EDT	[redacted] 1 restored (40.00 GB)	1:13pm EDT Apr 9 2013	14 minutes 5 seconds	40 gigabytes	0	0	Details

7. Once the restore is complete, the left column displays a green indicator (●) next to the restored data source.

How to Restore from a Replication Destination

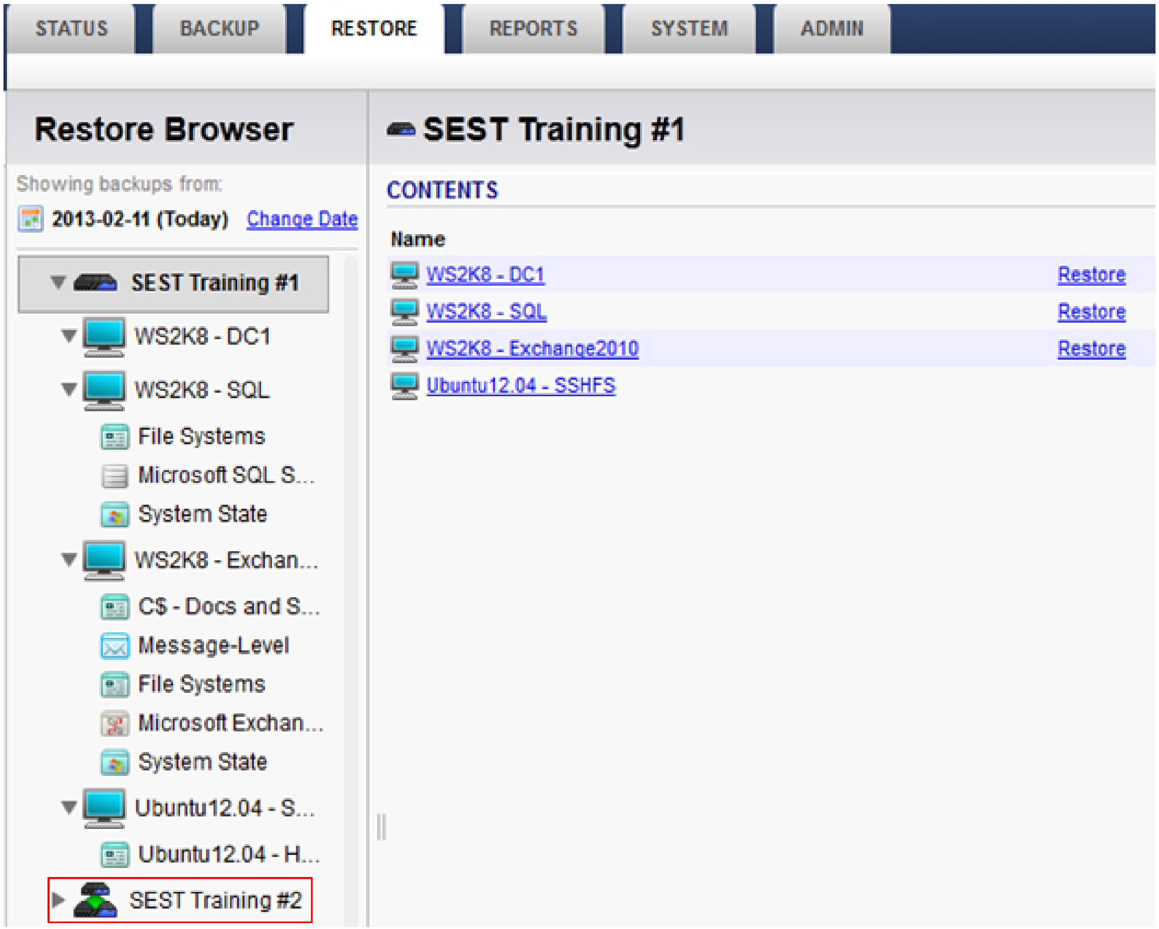
> This article refers to Barracuda Backup firmware 4.0 and higher, and assumes that replication has been successfully set up on both devices and that backups are running successfully.
>
> Only the Barracuda Backup Server 490 and higher can act as a backup to other Barracuda Backup Servers, although any Barracuda Backup Server can *send* data.

Related Articles

- Getting Started with Replication
- How to Restore a Microsoft SQL Database
- Microsoft SQL Server Database Recovery and Restoration
- How to Restore a Microsoft Exchange 2007 Database

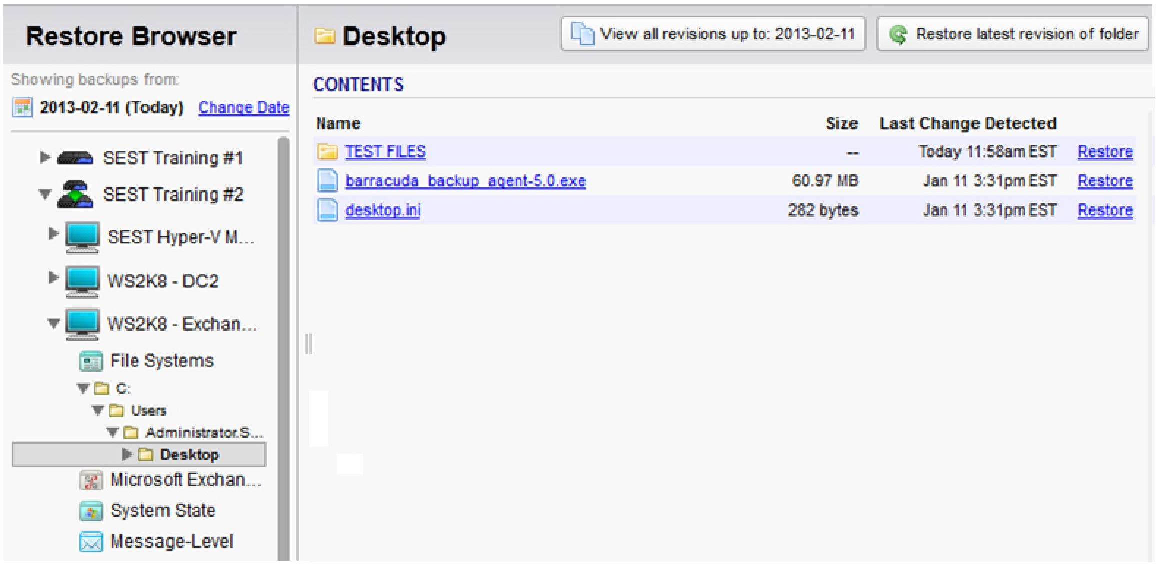
To restore from a replication destination,

1. Log into the Barracuda Backup web interface, and select the *receiving* Barracuda Backup Server from which to restore.
2. Go to the **Restore> Restore Browser** page, and in the left pane select the *sending* Barracuda Backup Server that you are receiving data from:



STATUS
BACKUP
RESTORE
REPORTS
SYSTEM
ADMIN
Restore Browser
Showing backups from:
2013-02-11 (Today)
Change Date
SEST Training #1
WS2K8 - DC1
WS2K8 - SQL
File Systems
Microsoft SQL S...
System State
WS2K8 - Exchan...
C$ - Docs and S...
Message-Level
File Systems
Microsoft Exchan...
System State
Ubuntu12.04 - S...
Ubuntu12.04 - H...
SEST Training #2
SEST Training #1
CONTENTS
Name
WS2K8 - DC1
Restore
WS2K8 - SQL
Restore
WS2K8 - Exchange2010
Restore
Ubuntu12.04 - SSHFS

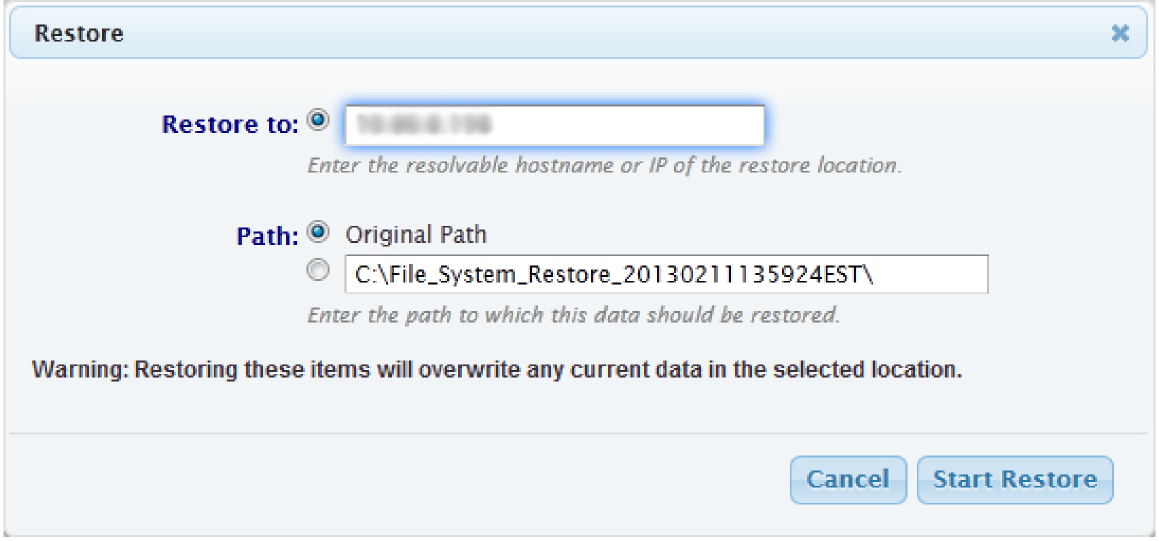
3. Expand the *sending* Barracuda Backup Server to review its backup sources, and click on the server or computer from which to restore; the contents displays in the right pane:


Restore Browser
Showing backups from:
2013-02-11 (Today)
Change Date
SEST Training #1
SEST Training #2
SEST Hyper-V M...
WS2K8 - DC2
WS2K8 - Exchan...
File Systems
C:
Users
Administrator.S...
Desktop
Microsoft Exchan...
System State
Message-Level
Desktop
View all revisions up to: 2013-02-11
Restore latest revision of folder

CONTENTS

Name	Size	Last Change Detected	
TEST FILES	--	Today 11:58am EST	Restore
barracuda_backup_agent-5.0.exe	60.97 MB	Jan 11 3:31pm EST	Restore
desktop.ini	282 bytes	Jan 11 3:31pm EST	Restore

4. In the **Contents** section, click **Restore** next to the file or directory for restore. The Restore window displays.
5. In the **Restore to** field, enter the hostname or IP address of the *restore to* location. In the **Path** section, select the **Original Path**, or you can designate a new location:


Restore
Cancel
Start Restore

Restore to: ● [redacted]
Enter the resolvable hostname or IP of the restore location.

Path: ● Original Path
○ C:\File_System_Restore_20130211135924EST\
Enter the path to which this data should be restored.

Warning: Restoring these items will overwrite any current data in the selected location.

6. Click **Start Restore**. Once the restore is complete, go to **REPORTS > Restore** to verify the restore completed successfully.

How to Restore SharePoint Objects Using Kroll Ontrack

This article refers to firmware version 5.4 and higher, Microsoft® SharePoint® 2010 and 2013, and Kroll® Ontrack® PowerControls ™ version 6.0 and later, and assumes you have an active Kroll Ontrack license.

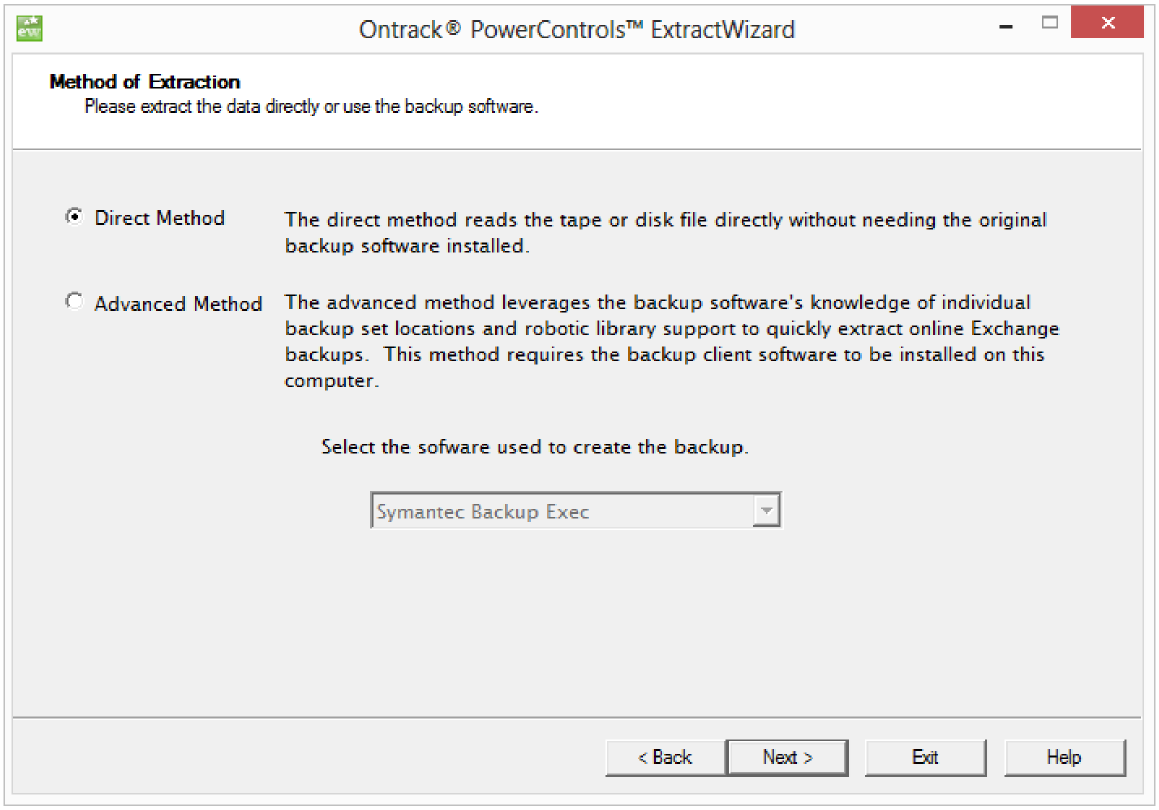
You can use Kroll Ontrack to granularly restore SharePoint Objects.

Restore SQL Flat File
To extract a SharePoint object from a restore, you must first restore the WSS_Content database to a flat file using the instructions in the article How to Restore a Microsoft SQL Server Database to a Flat File.

Extracting and Converting Files

Once you restore the content database using the instructions in the article How to Restore a Microsoft SQL Server Database to a Flat File, use the following steps to extract the **.bak** and **.trn** files, and then convert these files to **.mdf** and **.ldf** files.

1. Go to **Start > Programs > Kroll Ontrack > Ontrack PowerControls > PowerControls ExtractWizard**. On the introduction page of **ExtractWizard**, click **Next**.
2. In the **Method of Extraction** page, select **Direct Method:**



Method of Extraction

Please extract the data directly or use the backup software.

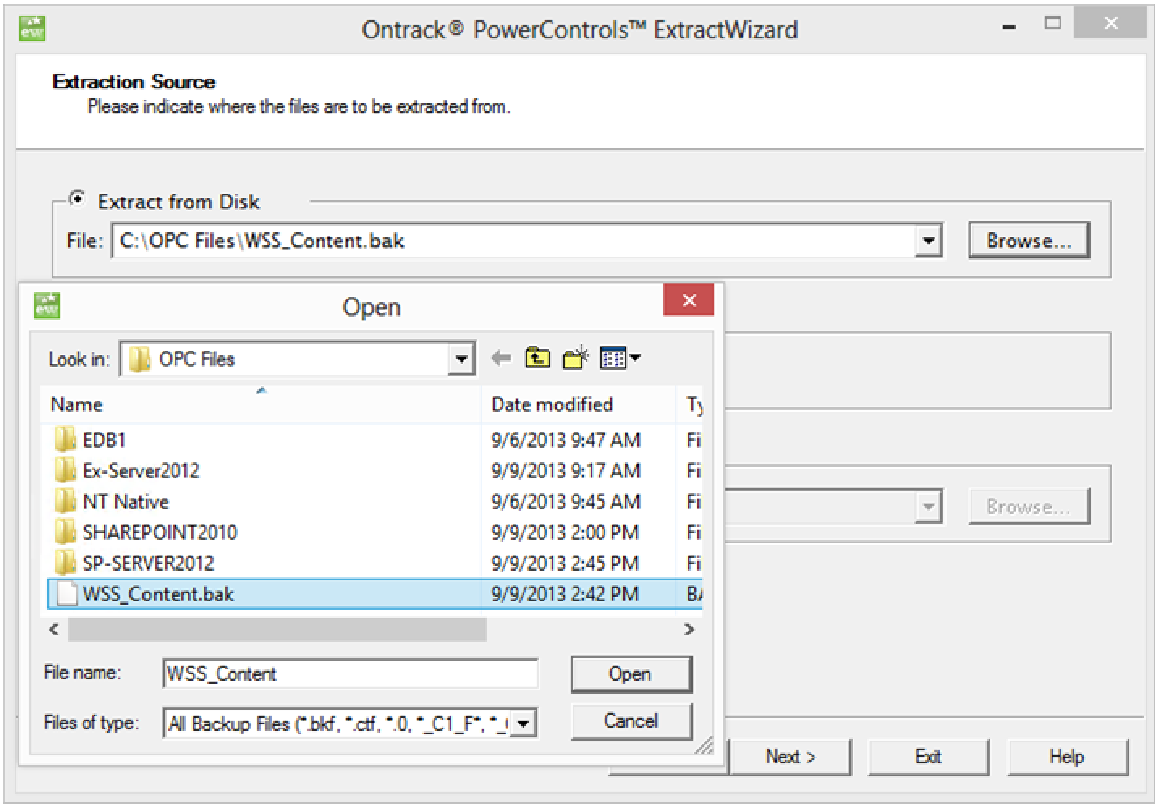
● Direct Method — The direct method reads the tape or disk file directly without needing the original backup software installed.

○ Advanced Method — The advanced method leverages the backup software's knowledge of individual backup set locations and robotic library support to quickly extract online Exchange backups. This method requires the backup client software to be installed on this computer.

Select the sofware used to create the backup.

Symantec Backup Exec

3. Click **Next**. On the **Extraction Source** page, navigate to and select the **.bak** file corresponding to the database you want to access:



Ontrack® PowerControls™ ExtractWizard

Extraction Source

Please indicate where the files are to be extracted from.

● Extract from Disk

File: C:\OPC Files\WSS_Content.bak

Open

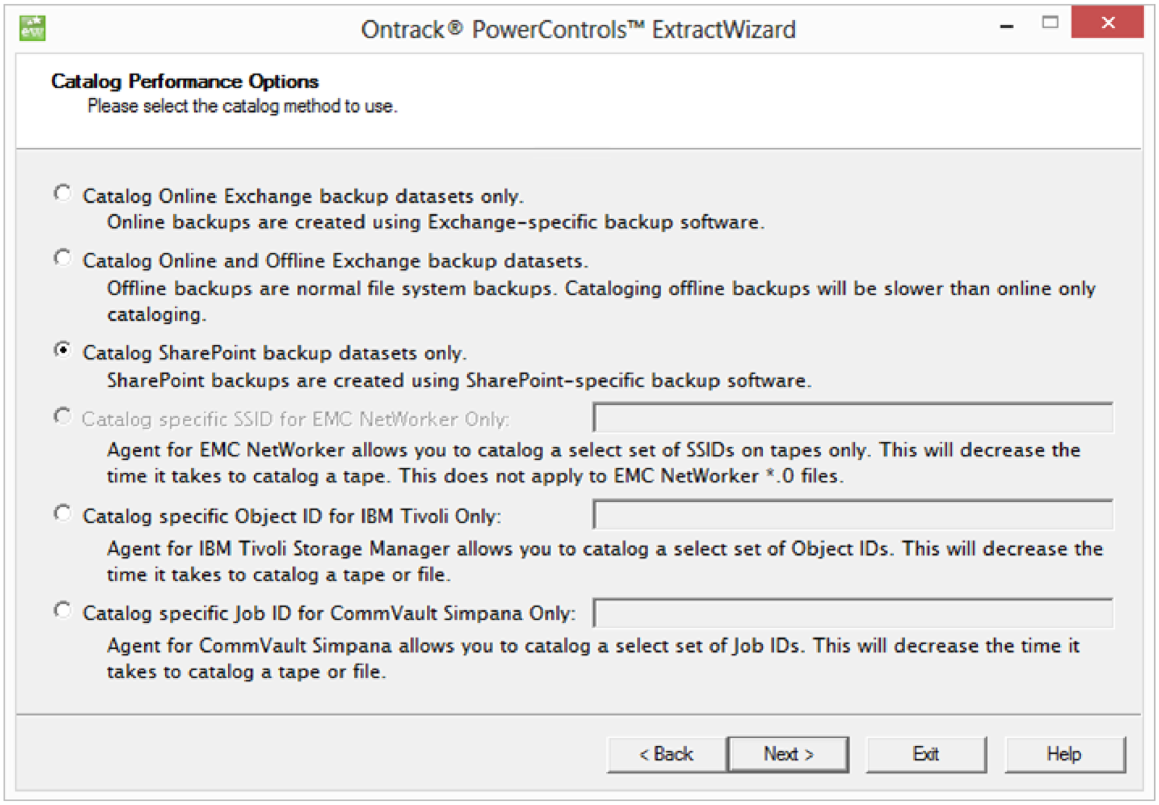
Look in: OPC Files

Name	Date modified	Ty
EDB1	9/6/2013 9:47 AM	Fi
Ex-Server2012	9/9/2013 9:17 AM	Fi
NT Native	9/6/2013 9:45 AM	Fi
SHAREPOINT2010	9/9/2013 2:00 PM	Fi
SP-SERVER2012	9/9/2013 2:45 PM	Fi
WSS_Content.bak	9/9/2013 2:42 PM	B/

File name: WSS_Content

Files of type: All Backup Files (*.bkf, *.ctf, *.0, *_C1_F*, *_(

4. Click **Next**. On the **Catalog Performance Options** page, select **Catalog SharePoint backup datasets only**:



Ontrack® PowerControls™ ExtractWizard

Catalog Performance Options

Please select the catalog method to use.

○ Catalog Online Exchange backup datasets only.
Online backups are created using Exchange-specific backup software.

○ Catalog Online and Offline Exchange backup datasets.
Offline backups are normal file system backups. Cataloging offline backups will be slower than online only cataloging.

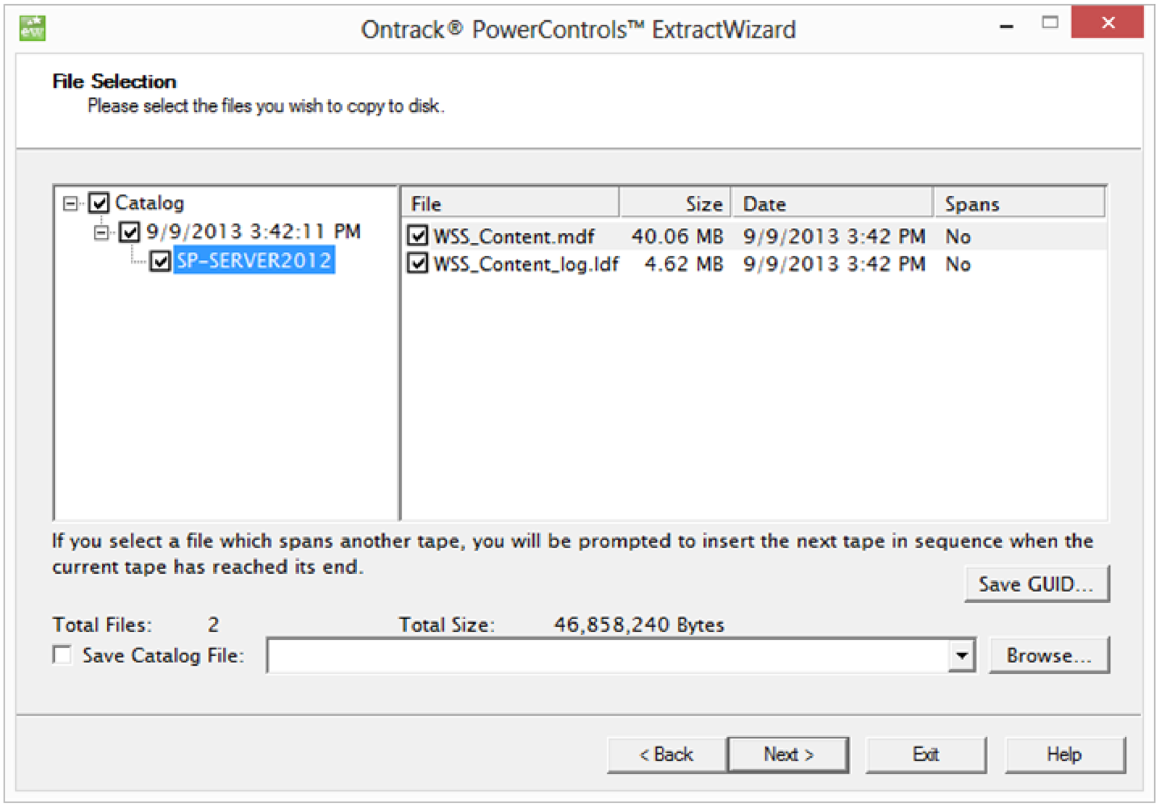
● Catalog SharePoint backup datasets only.
SharePoint backups are created using SharePoint-specific backup software.

○ Catalog specific SSID for EMC NetWorker Only:
Agent for EMC NetWorker allows you to catalog a select set of SSIDs on tapes only. This will decrease the time it takes to catalog a tape. This does not apply to EMC NetWorker *.0 files.

○ Catalog specific Object ID for IBM Tivoli Only:
Agent for IBM Tivoli Storage Manager allows you to catalog a select set of Object IDs. This will decrease the time it takes to catalog a tape or file.

○ Catalog specific Job ID for CommVault Simpana Only:
Agent for CommVault Simpana allows you to catalog a select set of Job IDs. This will decrease the time it takes to catalog a tape or file.

5. Click **Next**. On the **File Selection** page, select **Catalog**, or browse to and select the database set you want to recover:


Ontrack® PowerControls™ ExtractWizard
Save GUID...
Browse...
< Back
Next >
Exit
Help

File Selection

Please select the files you wish to copy to disk.

- ☑ Catalog
  - ☑ 9/9/2013 3:42:11 PM
    - ☑ SP-SERVER2012

File	Size	Date	Spans
☑ WSS_Content.mdf	40.06 MB	9/9/2013 3:42 PM	No
☑ WSS_Content_log.ldf	4.62 MB	9/9/2013 3:42 PM	No

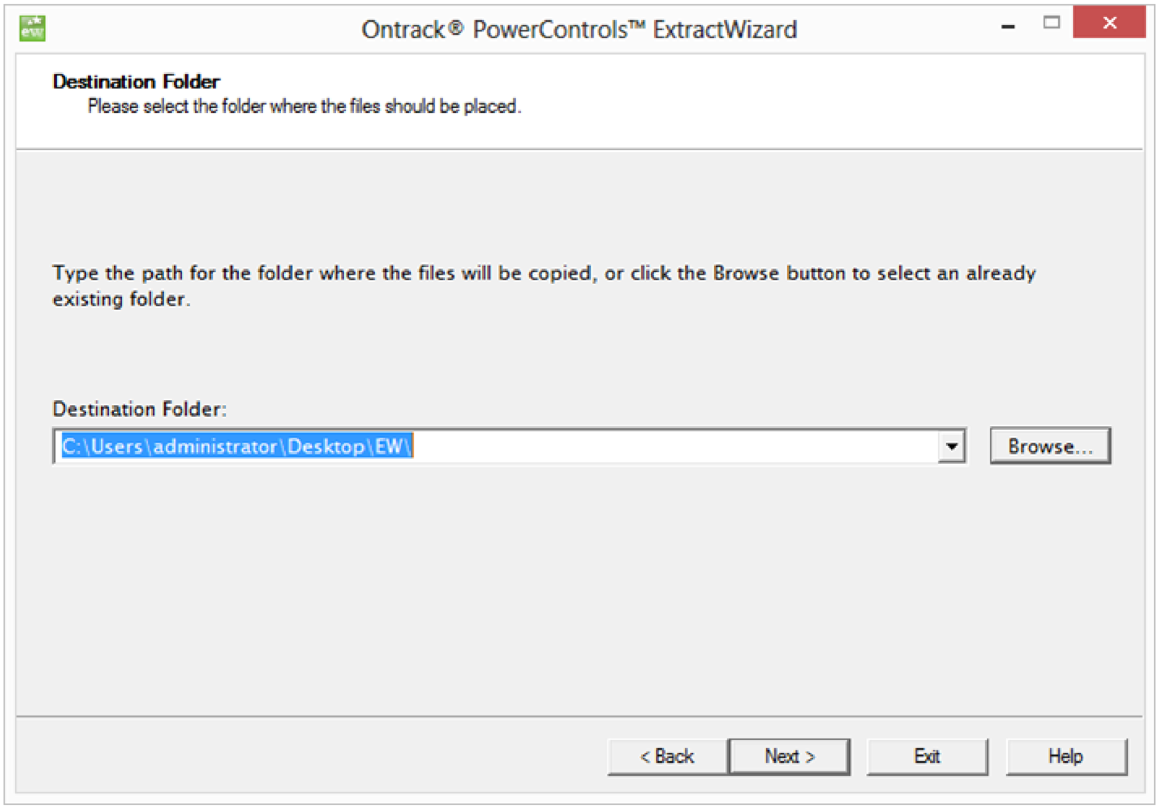
If you select a file which spans another tape, you will be prompted to insert the next tape in sequence when the current tape has reached its end.

Total Files: 2

Total Size: 46,858,240 Bytes

☐ Save Catalog File:

6. Click **Next**. On the **Destination Folder** page, browse to and select the destination folder where you want to copy the **.mdf** and **.ldf** files:


Ontrack® PowerControls™ ExtractWizard
Browse...
< Back
Next >
Exit
Help

Destination Folder

Please select the folder where the files should be placed.

Type the path for the folder where the files will be copied, or click the Browse button to select an already existing folder.

Destination Folder: C:\Users\administrator\Desktop\EW\

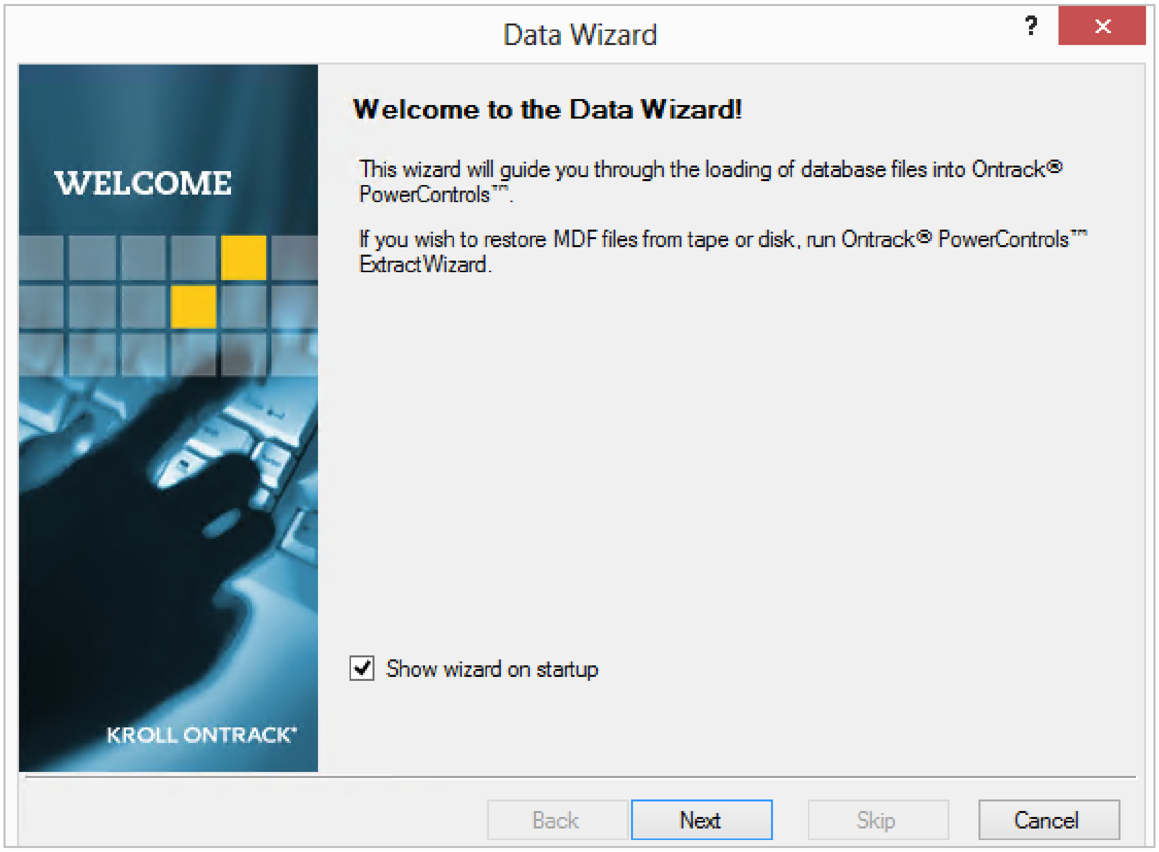
7. Click **Next**. Once the extraction is complete, click **Finish** to close **ExtractWizard**.

Restore the SharePoint Objects

Once you extract the **.mdf** and **.ldf** files from the restore, use the following steps to browse to and restore the SharePoint objects.

1. Go to **Start > Programs > Kroll Ontrack > Ontrack PowerControls > PowerControls for SharePoint**. The **Data Wizard** displays

:


Data Wizard
?
✕
WELCOME
KROLL ONTRACK
Back
Next
Skip
Cancel

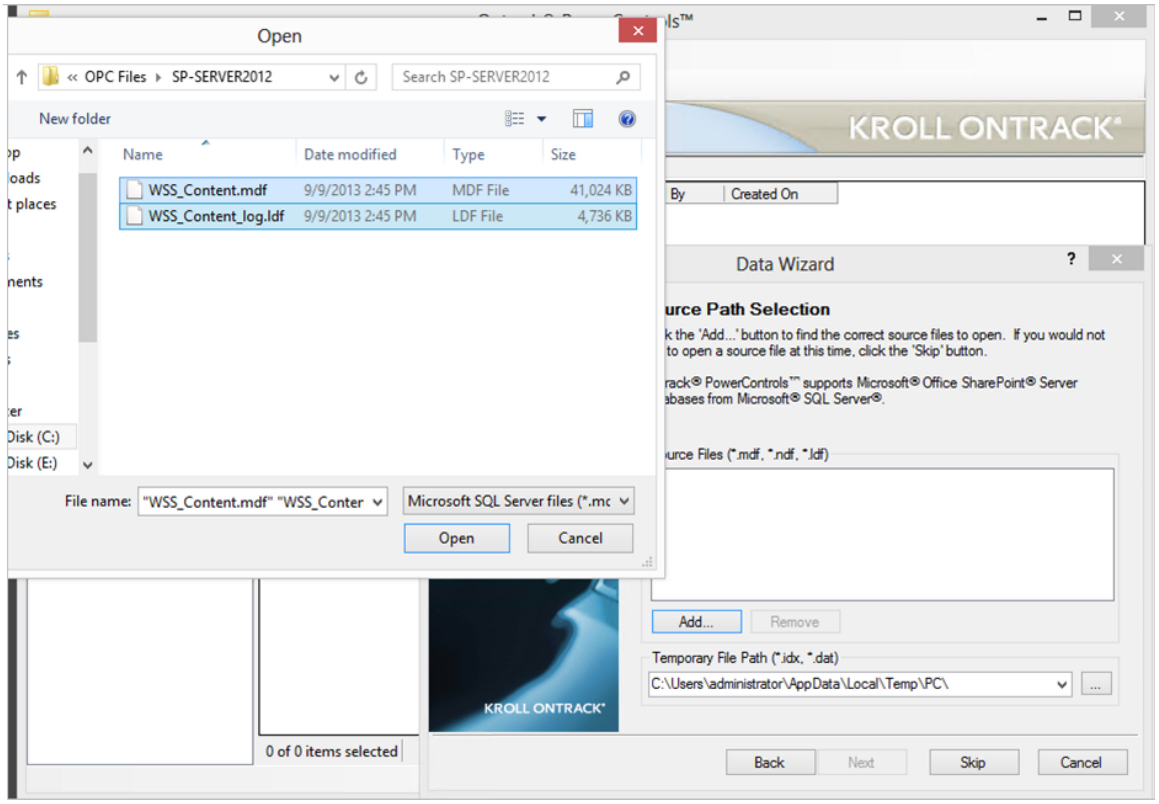
Welcome to the Data Wizard!

This wizard will guide you through the loading of database files into Ontrack® PowerControls™.

If you wish to restore MDF files from tape or disk, run Ontrack® PowerControls™ ExtractWizard.

☑ Show wizard on startup

2. Click **Next**. In the **Source Path Selection** page, click **Add**, and navigate to and select the files created using the **ExtractWizard** in the previous section:


Open
OPC Files ▸ SP-SERVER2012
Search SP-SERVER2012
New folder
Name
Date modified
Type
Size
KROLL ONTRACK
By
Created On
Data Wizard
Add...
Remove
Back
Next
Skip
Cancel
Open
Cancel
KROLL ONTRACK
0 of 0 items selected

Name	Date modified	Type	Size
WSS_Content.mdf	9/9/2013 2:45 PM	MDF File	41,024 KB
WSS_Content_log.ldf	9/9/2013 2:45 PM	LDF File	4,736 KB

File name: "WSS_Content.mdf" "WSS_Conter

Microsoft SQL Server files (*.mc

urce Path Selection

k the 'Add...' button to find the correct source files to open. If you would not to open a source file at this time, click the 'Skip' button.

rack® PowerControls™ supports Microsoft® Office SharePoint® Server abases from Microsoft® SQL Server®.

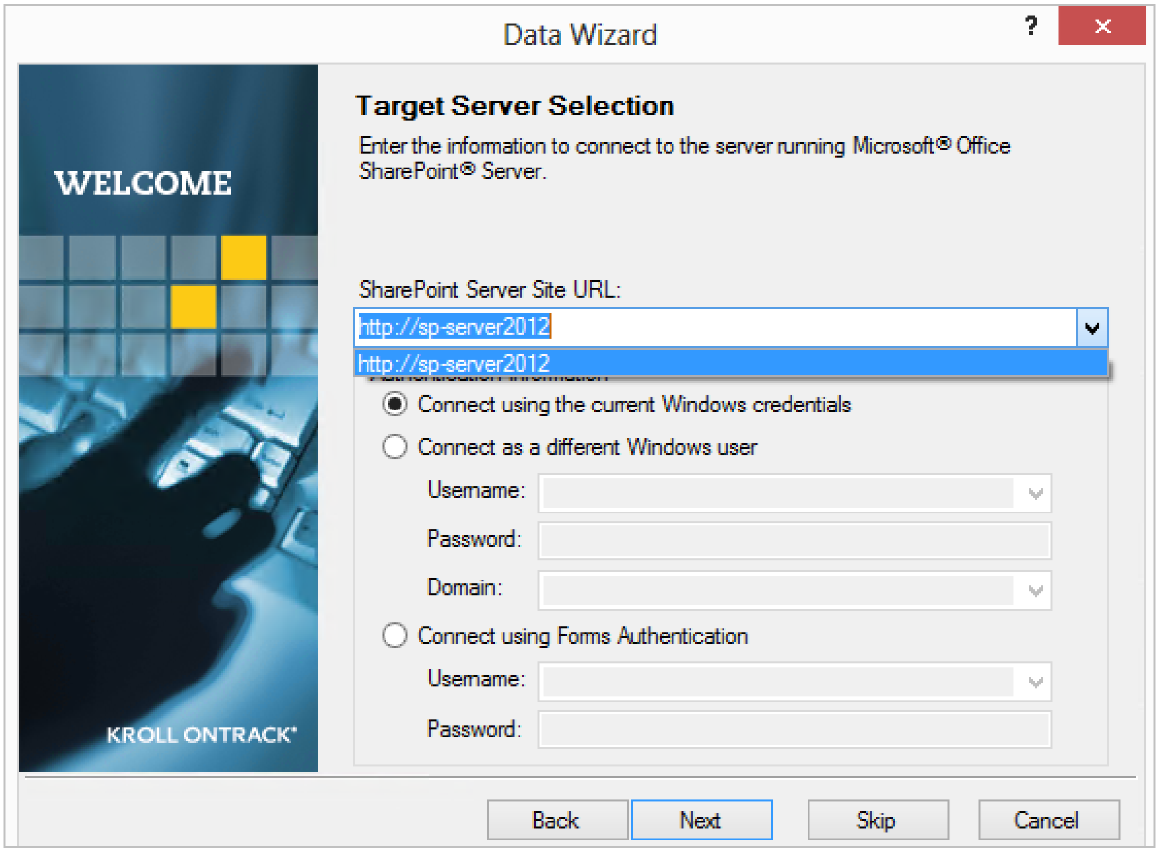
urce Files (*.mdf, *.ndf, *.ldf)

Temporary File Path (*.idx, *.dat)

C:\Users\administrator\AppData\Local\Temp\PC\

3. Click **Open** to add the files. Verify the **Temporary File Path** is valid, and then click **Next**.
4. The database content displays in the **Source** list.

5. In the **Target Server Selection** page, from the **SharePoint Server Site URL** drop-down menu, select the *target* site URL:



Data Wizard

Target Server Selection

Enter the information to connect to the server running Microsoft® Office SharePoint® Server.

SharePoint Server Site URL: http://sp-server2012

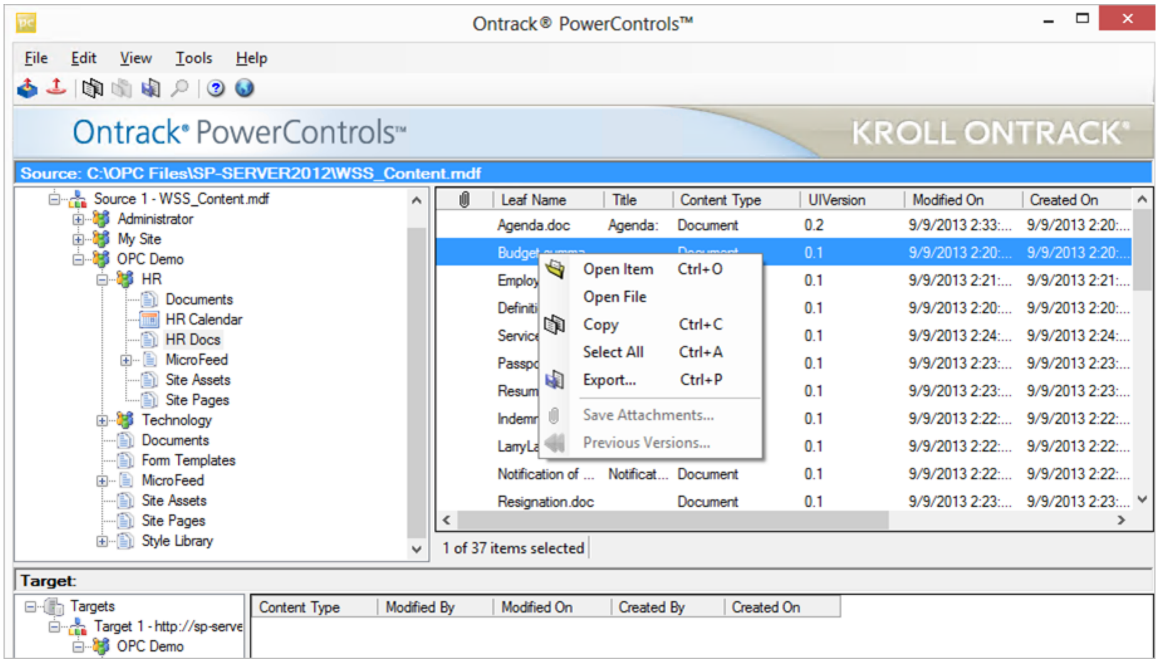
● Connect using the current Windows credentials

○ Connect as a different Windows user

○ Connect using Forms Authentication

WELCOME
KROLL ONTRACK®
http://sp-server2012
Username:
Password:
Domain:
Username:
Password:
Back
Next
Skip
Cancel

6. Select an authentication option, and then click **Next**.
7. The *source* and *target* selections display. Expand the **Source** list, right click the item to restore, and then click **Copy**:



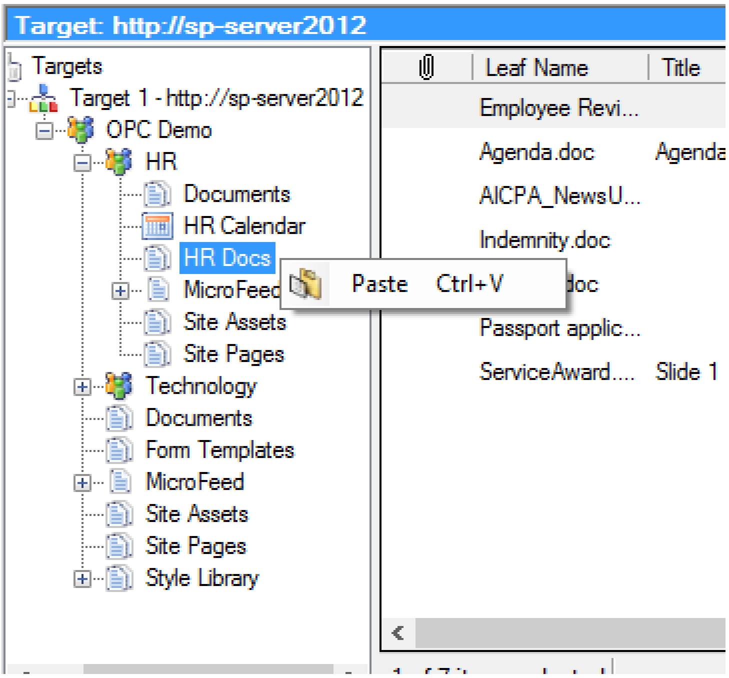
Ontrack® PowerControls™

Source: C:\OPC Files\SP-SERVER2012\WSS_Content.mdf

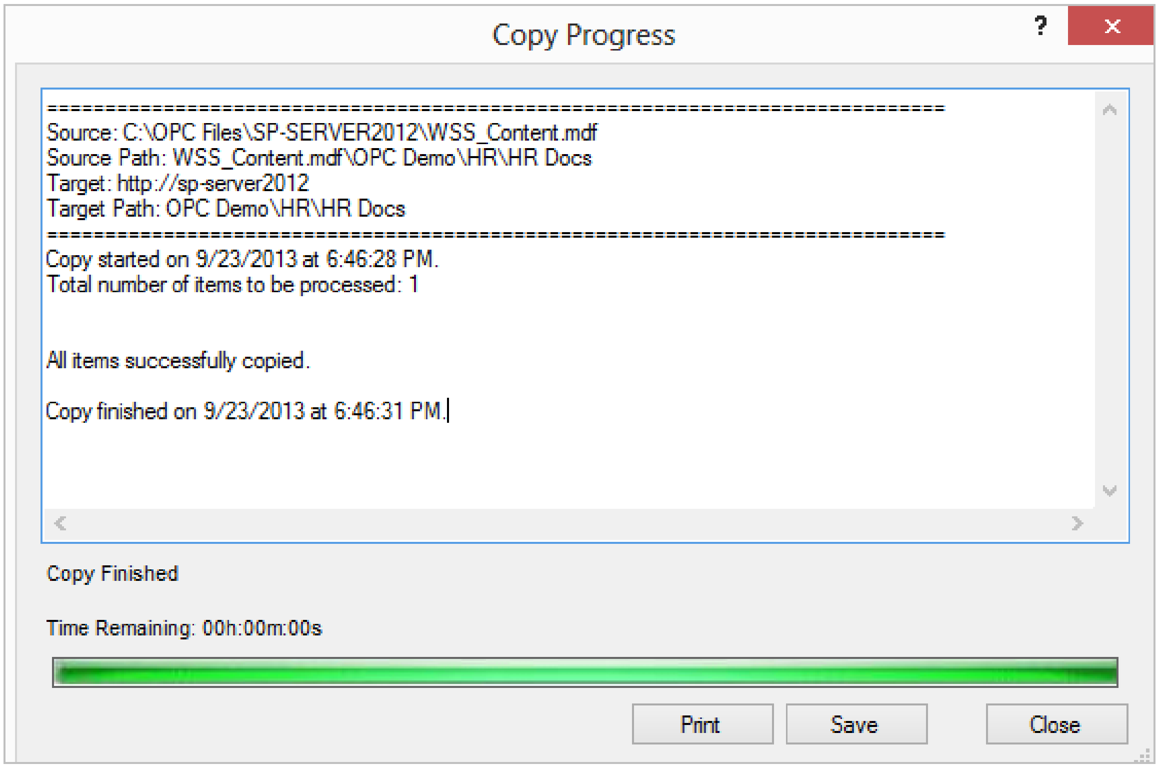
1 of 37 items selected

File
Edit
View
Tools
Help
Ontrack® PowerControls™
KROLL ONTRACK®
Source 1 - WSS_Content.mdf
Administrator
My Site
OPC Demo
HR
Documents
HR Calendar
HR Docs
MicroFeed
Site Assets
Site Pages
Technology
Documents
Form Templates
MicroFeed
Site Assets
Site Pages
Style Library
Leaf Name
Title
Content Type
UIVersion
Modified On
Created On
Agenda.doc
Budget summa...
Employ
Definiti
Servic
Passpo
Resum
Indemn
LarryLa
Notification of ...
Resignation.doc
Open Item Ctrl+O
Open File
Copy Ctrl+C
Select All Ctrl+A
Export... Ctrl+P
Save Attachments...
Previous Versions...
Target:
Targets
Target 1 - http://sp-serve
OPC Demo
Content Type
Modified By
Modified On
Created By
Created On

8. Expand the **Target** list, right-click the the site object location where you want to copy the source file, and click **Paste**:


Target: http://sp-server2012
Targets
Target 1 - http://sp-server2012
OPC Demo
HR
Documents
HR Calendar
HR Docs
MicroFeed
Site Assets
Site Pages
Technology
Documents
Form Templates
MicroFeed
Site Assets
Site Pages
Style Library
Leaf Name
Title
Employee Revi...
Agenda.doc
Agenda
AICPA_NewsU...
Indemnity.doc
doc
Passport applic...
ServiceAward....
Slide 1
Paste Ctrl+V

9. Once the restore process is complete, the **Copy Progress** status log generates:


Copy Progress
?
✕

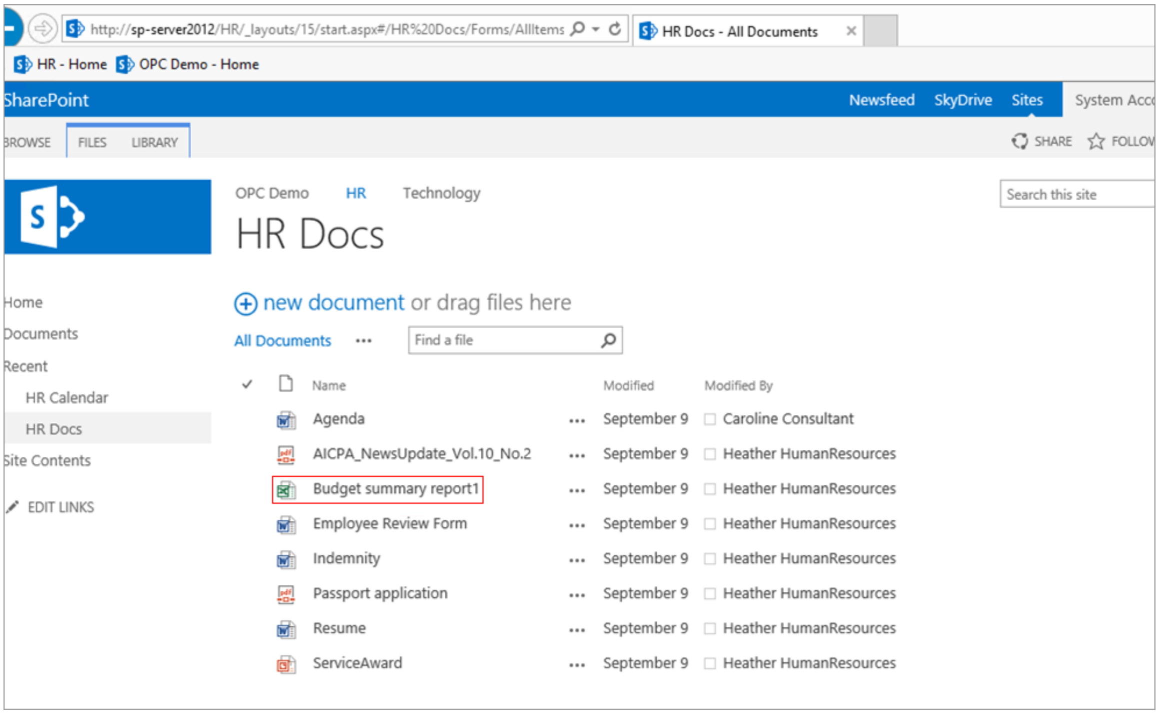
```
================================================================================
Source: C:\OPC Files\SP-SERVER2012\WSS_Content.mdf
Source Path: WSS_Content.mdf\OPC Demo\HR\HR Docs
Target: http://sp-server2012
Target Path: OPC Demo\HR\HR Docs
================================================================================
Copy started on 9/23/2013 at 6:46:28 PM.
Total number of items to be processed: 1


All items successfully copied.

Copy finished on 9/23/2013 at 6:46:31 PM.
```

Copy Finished

Time Remaining: 00h:00m:00s

Print
Save
Close

10. Click **Print** to print a copy of the report, **Save** to save a copy to your local system, or click **Close**.
11. Log in to SharePoint and verify the object has been restored to the desired location:


http://sp-server2012/HR/_layouts/15/start.aspx#/HR%20Docs/Forms/AllItems
HR Docs - All Documents
HR - Home
OPC Demo - Home
SharePoint
Newsfeed
SkyDrive
Sites
System Acc
BROWSE
FILES
LIBRARY
SHARE
FOLLOW
OPC Demo
HR
Technology
HR Docs
Search this site
Home
Documents
Recent
HR Calendar
HR Docs
Site Contents
EDIT LINKS
new document or drag files here
All Documents
Find a file

Name		Modified	Modified By
Agenda	•••	September 9	Caroline Consultant
AICPA_NewsUpdate_Vol.10_No.2	•••	September 9	Heather HumanResources
Budget summary report1	•••	September 9	Heather HumanResources
Employee Review Form	•••	September 9	Heather HumanResources
Indemnity	•••	September 9	Heather HumanResources
Passport application	•••	September 9	Heather HumanResources
Resume	•••	September 9	Heather HumanResources
ServiceAward	•••	September 9	Heather HumanResources

How to Restore a Microsoft Windows Server 2003 Domain Controller

Additional Resource
- Restart the domain controller in Directory Services Restore Mode Remotely

Use the following steps to restore a Windows Server:

1. Log in to the Windows Server, and reboot the server into directory services restore mode.

> **Remotely Reboot**
> Note that you can reboot the server remotely; for more information, refer to the Microsoft TechNet article Restart the domain controller in Directory Services Restore Mode Remotely.

2. Log in to the Barracuda Backup web interface, select the associated Barracuda Backup Server in the left pane, and go to the **BACKUPS > Restore** page.
3. Under the domain controller on the left, click **System State**.
4. Click **Restore** next to the date from which to restore.
5. In the dialog box, select either the original location or an alternate location, and turn on **Authoritative Restore.**

> You must turn on **Authoritative Restore** for your changes to be replicated.

6. Click **Start Restore**, and then click **OK**.
7. Go to the **REPORTS > Restore** page to view restore progress.
8. Log back in to the Windows Server, and reboot the domain controller into normal mode.
9. The restore is now complete.

Best Practice
Test replication after a restore if you have more than one domain controller.

How to Restore Windows System State

Restoring Windows System State should only be performed in a disaster recovery situation. Typically, this is if a server goes down and will not boot or if the configuration is severely corrupted.

In this Section

- How to Restore Windows Server 2003 Domain Controller System State
- How to Restore Windows Server 2008 Domain Controller System State

How to Restore Windows Server 2003 Domain Controller System State

> This article refers to Barracuda Backup firmware version 3.1 and higher, and Windows® Server 2003 domain controller. This article assumes that a System State backup exists, and that the user restoring to System State has access to the Directory Services Restore Mode (DSRM) password. If you are restoring Windows Server 2008, refer to the article How to Restore Windows Server 2008 Domain Controller System State. You cannot perform a system state restore from the Cloud.

In this article:

- Requirements
- Active Directory Domain Controllers
- Prepare the Target
- Restore File System and System State
- Restore System State

Related Articles
- Barracuda Backup Agent (Windows) - Restore Windows Server 2008 Domain Controller System State

Additional Resources
- Active Directory Backup and Restore

Disaster Recovery
Restoring Windows System State should only be performed in a disaster recovery situation. Typically, this is if a server goes down and will not boot, or if the configuration is severely corrupted.

Requirements

Before proceeding, verify that all of the following are true:

- The Barracuda Backup Agent is installed on the *target* server;
- File System and System State from the *source* server exist;
- Both the *target* and *source* server hardware and operating systems are configured the same; and
- The *target* server is on the network and can communicate directly with the Barracuda Backup Server.

Active Directory Domain Controllers

For Active Directory (AD) domain controllers, you must have access to the DSRM password. Additionally, it is *highly recommended* that the IP address to which you are restoring is the same as the original server.

Prepare the Target

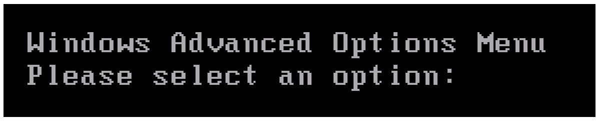
When setting up the *target* server, the configuration should be identical to that of the *source* server that you are restoring including:

- Version
- Edition

- 32- or 64-bit

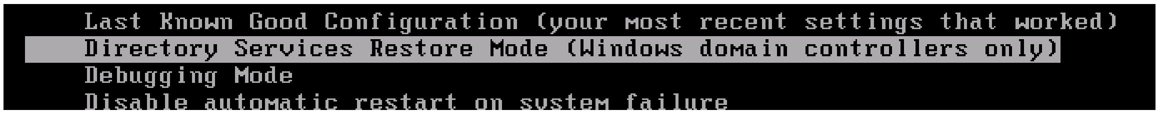
For example, if the *source* server is 64-bit Windows 2003 R2, Enterprise Edition, the *target* server should also be 64-bit Windows 2003 R2, Enterprise Edition.

1. Power on the *target* server, or if it is already running, reboot the *target* server.
2. Once the *target* server boots up, hold down the **F8** key until the Windows Advanced Options menu displays:



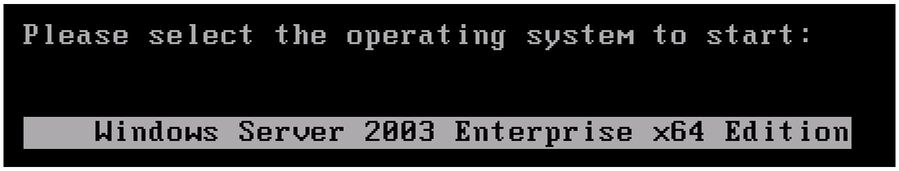
```
Windows Advanced Options Menu
Please select an option:
```

3. Use the **Arrow** keys on the keyboard to select the **Directory Services Restore Mode**:



```
    Last Known Good Configuration (your most recent settings that worked)
    Directory Services Restore Mode (Windows domain controllers only)
    Debugging Mode
    Disable automatic restart on system failure
```

4. Press **Enter**. The **Select Operating System to Boot** menu displays; Select the appropriate operating system:

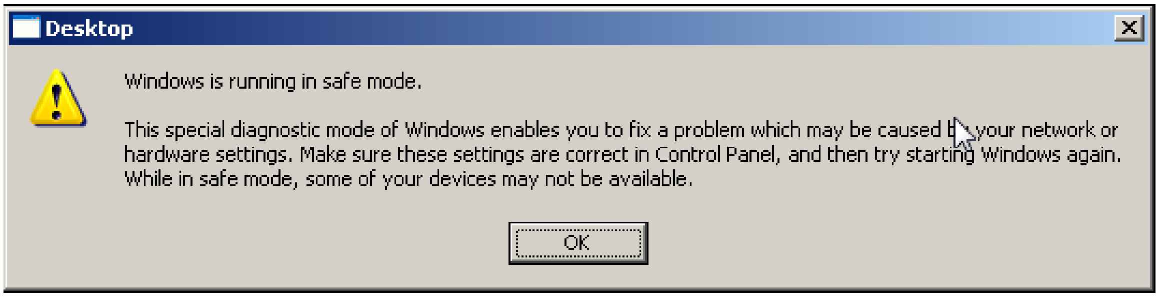


```
Please select the operating system to start:


    Windows Server 2003 Enterprise x64 Edition
```

5. Press **Enter**. Windows reboots in **Directory Services Restore Mode**; **Safe Mode** displays onscreen:

```
Safe Mode
```

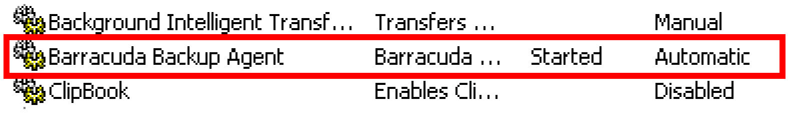
6. When the log in prompt appears, press **Ctrl-Alt Delete** and log in to Windows using the administrator account.
7. The **Safe Mode** warning dialog displays:



Windows is running in safe mode.

This special diagnostic mode of Windows enables you to fix a problem which may be caused by your network or hardware settings. Make sure these settings are correct in Control Panel, and then try starting Windows again. While in safe mode, some of your devices may not be available.

8. Click **OK** to close the dialog and continue in Safe Mode.
9. Click **Start > Run**, enter **services.msc**, and click **OK** to open **Services**.
10. Navigate to **Barracuda Backup Agent** in the list of Services and verify the **Status** field displays as **Started**:



Background Intelligent Transf...	Transfers ...		Manual
Barracuda Backup Agent	Barracuda ...	Started	Automatic
ClipBook	Enables Cli...		Disabled

> If the Barracuda Backup Agent Service is *not* listed in the Services window, you must first install the Agent before proceeding.

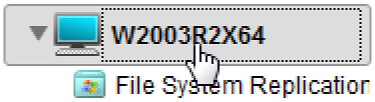
11. If the **Status** field displays as **Stopped**, right click the Agent, and click **Start**.

Restore File System and System State

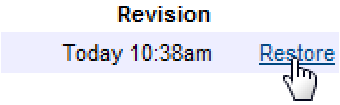
Use the following steps to restore an AD domain controller to the *target* server, or to restore a complete copy of the *source* server without AD.

> This procedure restores the file system, overwriting existing files. Restoring System State from a *source* domain controller restores AD to its original state on that server; check with your system administrator before restoring a domain controller from an old revision backup.

1. Log in to the Barracuda Backup web interface, and go to **RESTORE > Restore Browser**.
2. Select the Windows Server that represents the *source* server you wish to restore:



3. Click **View all revisions up to: <date>**; a list of revisions displays.
4. Click **Restore** next to the revision you wish to restore:

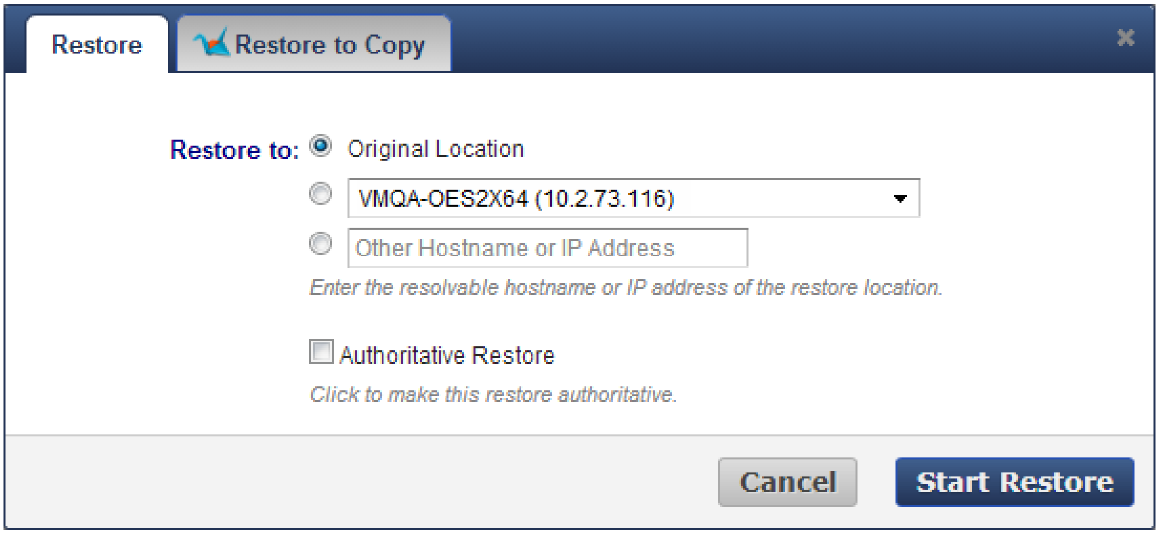


Revision	
Today 10:38am	Restore

5. The **Restore** window displays.

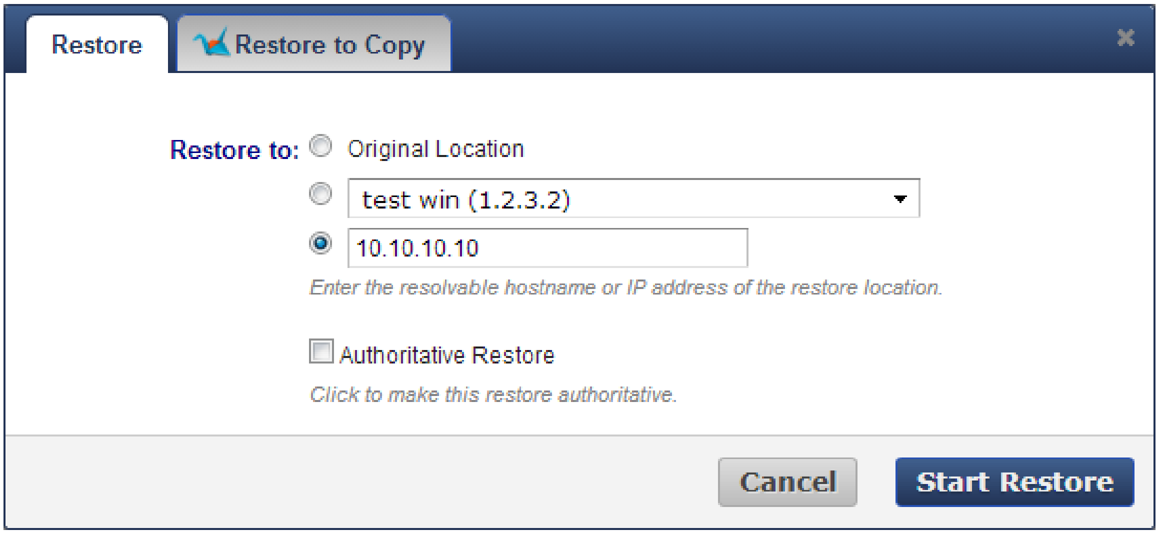
> ⚠ **Authoritative Restore**
> An authoritative restore returns the source server to the state it was in at the time of the backup, overwriting all changes made since that backup was performed. Changes made subsequent to that backup will be lost. For more information on authoritative restore, refer to the Microsoft TechNet article Active Directory Backup and Restore.

If the *target* server is set up with the same IP address as the *source* server you are restoring, select **Original Location**:



Restore to: ● Original Location
○ VMQA-OES2X64 (10.2.73.116)
○ Other Hostname or IP Address
Enter the resolvable hostname or IP address of the restore location.
☐ Authoritative Restore
Click to make this restore authoritative.

If the *target* server has a different IP address, select the third option and enter the IP address of the new location:



Restore to: ○ Original Location
○ test win (1.2.3.2)
● 10.10.10.10
Enter the resolvable hostname or IP address of the restore location.
☐ Authoritative Restore
Click to make this restore authoritative.

6. Click **Start Restore**.
7. Go to **REPORTS > Restore** to view restore job details.

> ⓘ **Restore Job**

The restore job completion is dependent upon the size of the original server.

8. Once the restore is complete, a dialog displays. Click **OK** to close the dialog box.
9. Once the restore job is complete, restart the server.

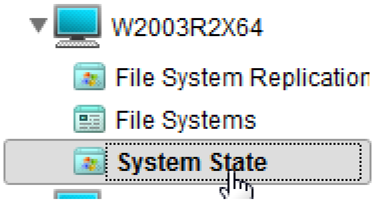
Restore System State

Use the procedure described in this section *only* if you wish to restore System State to the *target* server without restoring the rest of the file system as it was on the *source* server. This procedure restores System files including those in the **C:\Windows** folder. Perform the steps in this section if you are *not* performing full disaster recovery and wish to keep the *target* server's file system intact. Since this procedure does not restore file systems, following these steps will not restore replicated file systems or administration tools if the *source* server was a domain controller. This means group policy objects and log on scripts will not be available on the *target* server unless they are already on that server or on another server on the network. If you wish to restore file systems, use the steps described in the section Restoring File System and System State, or restore file systems manually from another server on the network.

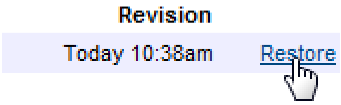
> ⚠ **Important**
> Restoring System State from a *source* domain controller restores AD to its original state on that server; check with your system administrator before restoring a domain controller from an old revision backup.

To restore System State only,

1. Log in to the Barracuda Backup web interface, and go to **RESTORE > Restore Browser**.
2. Expand the Windows Server that represents the *source* server, and select **System State**:



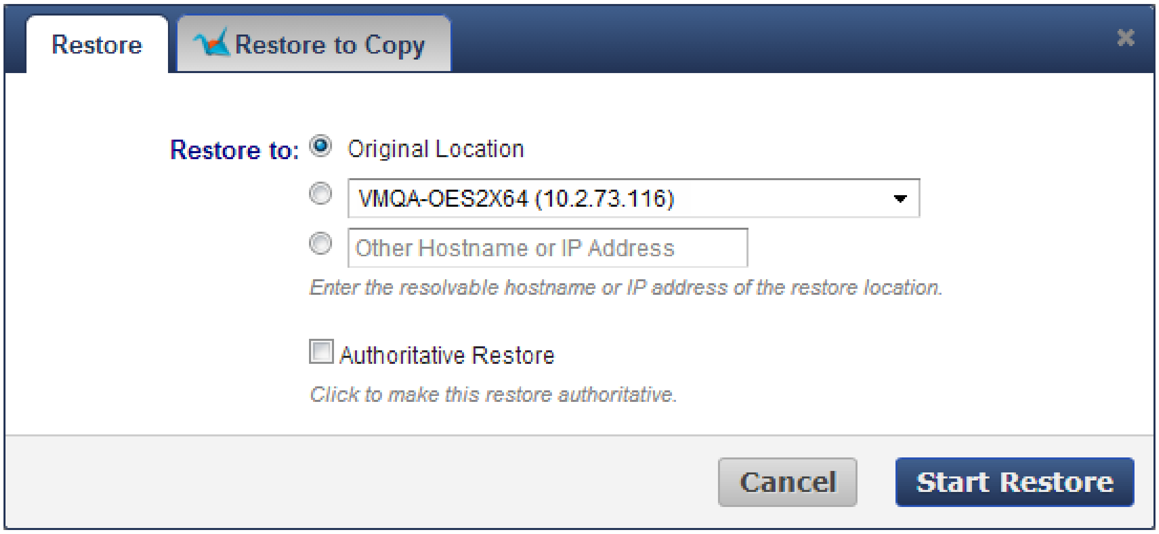
3. Click **View all revisions up to: <date>**; a list of revisions displays.
4. Click **Restore** next to the revision you wish to restore:



5. The **Restore** window displays.

> ⚠ **Authoritative Restore**
> An authoritative restore returns the *source* server to the state it was in at the time of the backup, overwriting all changes made since that backup was performed. Changes made subsequent to that backup will be lost. For more information on authoritative restore, refer to the Microsoft TechNet article Active Directory Backup and Restore.

If the *target* server is set up with the same IP address as the *source* server you are restoring, select **Original Location**:



Restore to: ● Original Location

○ VMQA-OES2X64 (10.2.73.116)

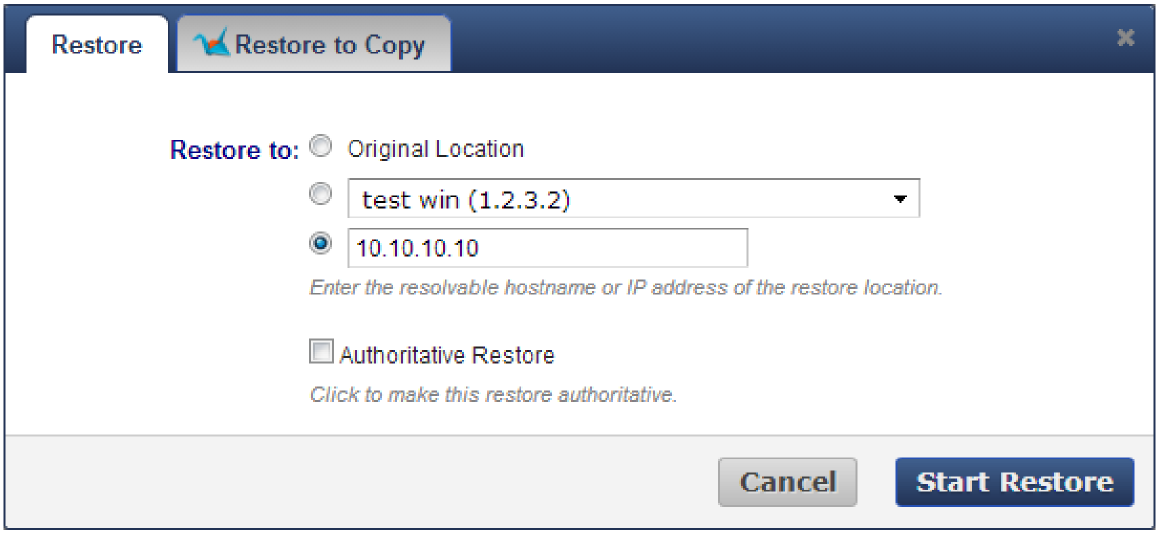
○ Other Hostname or IP Address

Enter the resolvable hostname or IP address of the restore location.

☐ Authoritative Restore

Click to make this restore authoritative.

If the *target* server has a different IP address, select the third option and enter the IP address of the new location:



Restore to: ○ Original Location

○ test win (1.2.3.2)

● 10.10.10.10

Enter the resolvable hostname or IP address of the restore location.

☐ Authoritative Restore

Click to make this restore authoritative.

6. Click **Start Restore**.
7. Go to **REPORTS > Restore** to view restore job details.

> **Restore Job**
> The restore job completion is dependent upon the size of the original server.

8. Once the restore is complete, a dialog displays. Click **OK** to close the dialog box.
9. Once the restore job is complete, restart the server.

How to Restore Windows Server 2008 Domain Controller System State

> This article refers to Barracuda Backup firmware version 3.1 and higher, and Windows ® Server 2008 domain controller. This article assumes that a System State backup exists, and that the user restoring to System State has access to the Directory Services Restore Mode (DSRM) password. If you are restoring Windows Server 2003, refer to the article How to Restore Windows Server 2003 Domain Controller System State. You cannot perform a system state restore from the Cloud.

In this article:

- Requirements
- Active Directory Domain Controllers
- Prepare the Target
- Restore File System and System State
- Restore System State
- Restore Normal Boot Mode

Related Articles

- Barracuda Backup Agent
- Restore Windows Server 2003 Domain Controller System State

Additional Resources

- Active Directory Backup and Restore

Disaster Recovery
Restoring Windows System State should only be performed in a disaster recovery situation. Typically, this is if a server goes down and will not boot, or if the configuration is severely corrupted.

Requirements

Before proceeding, verify that all of the following are true:

- The Barracuda Backup Agent is installed on the *target server*;
- File System and System State from the *source* server exist;
- Both the *target* and *source* server hardware and operating systems are configured the same; and
- The *target* server is on the network and can communicate directly with the Barracuda Backup Server.

Active Directory Domain Controllers

For Active Directory (AD) domain controllers, you must have access to the DSRM password. Additionally, it is *highly recommended* that the IP address to which you are restoring is the same as the original server.

Prepare the Target

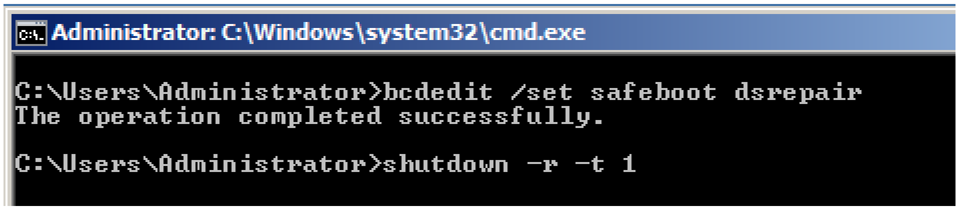
When setting up the *target* server, the configuration should be identical to that of the *source* server that you are restoring including:

- Version
- Edition
- 32- or 64-bit

For example, if the *source* server is 32-bit Windows 2008, Enterprise Edition, the *target* server should also be 32-bit Windows 2008, Enterprise Edition.

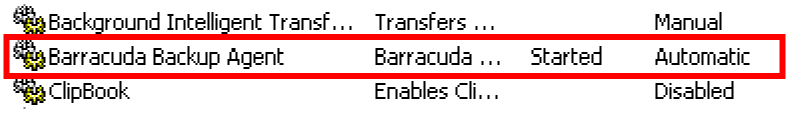
Cancel Restore
If you decide you do not wish to restore the server, use the steps in the section Restoring Normal Boot Mode to return your server to the normal boot mode.

1. Power on the *target* server, or if it is already running, reboot the *target* server.
2. Log on using an administrator account; if the *target* server is a domain controller, log in using a domain account with administrative access to the server.
3. At a command prompt, enter the following command:
   ```
   bcdedit /set safeboot dsrepair
   ```
4. Press **Enter**, and then enter the following command to restart the server:
   ```
   shutdown -r -t 1
   ```



```
C:\Users\Administrator>bcdedit /set safeboot dsrepair
The operation completed successfully.

C:\Users\Administrator>shutdown -r -t 1
```

5. Press **Enter** to restart the server. The server restarts, and Windows boots into Directory Services Repair Mode.
6. Press **Ctrl-Alt-Delete** and log into the system using the same credentials you entered above in **Step 2**.
7. Click **Start > Run** , enter **services.msc** , and click **OK** to open **Services** .
8. Navigate to **Barracuda Backup Agent** in the list of Services, and verify the **Status** field displays as **Started** :



Background Intelligent Transf...	Transfers ...		Manual
Barracuda Backup Agent	Barracuda ...	Started	Automatic
ClipBook	Enables Cli...		Disabled

> ⓘ If the Barracuda Backup Agent Service is *not* listed in the Services window, you must first install the Agent before proceeding.

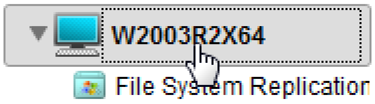
9. If the **Status** field displays as **Stopped**, right click the Agent, and click **Start**.

Restore File System and System State

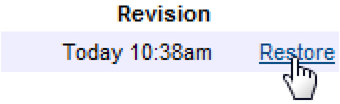
Use the following steps to restore an AD domain controller to the *target* server, or to restore a complete copy of the *source* server without AD.

> ⚠ This procedure restores the file system, overwriting existing files. Restoring System State from a *source* domain controller restores AD to its original state on that server; check with your system administrator before restoring a domain controller from an old revision backup.

1. Log in to the Barracuda Backup web interface, and go to **RESTORE > Restore Browser**.
2. Select the Windows Server that represents the *source* server you wish to restore:



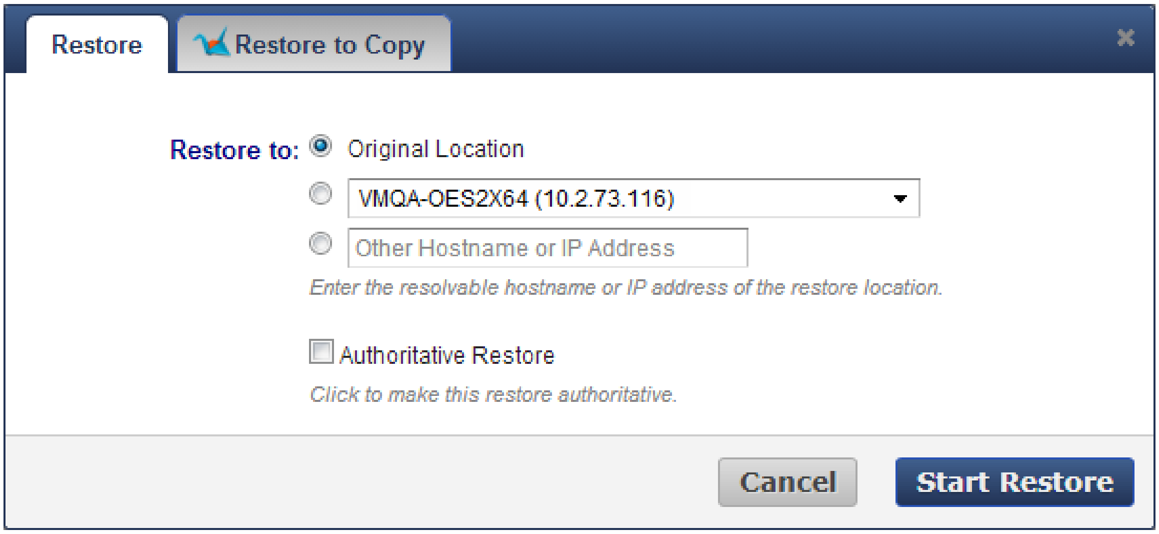
3. Click **View all revisions up to: <date>**; a list of revisions displays.
4. Click **Restore** next to the revision you wish to restore:



5. The **Restore** window displays.

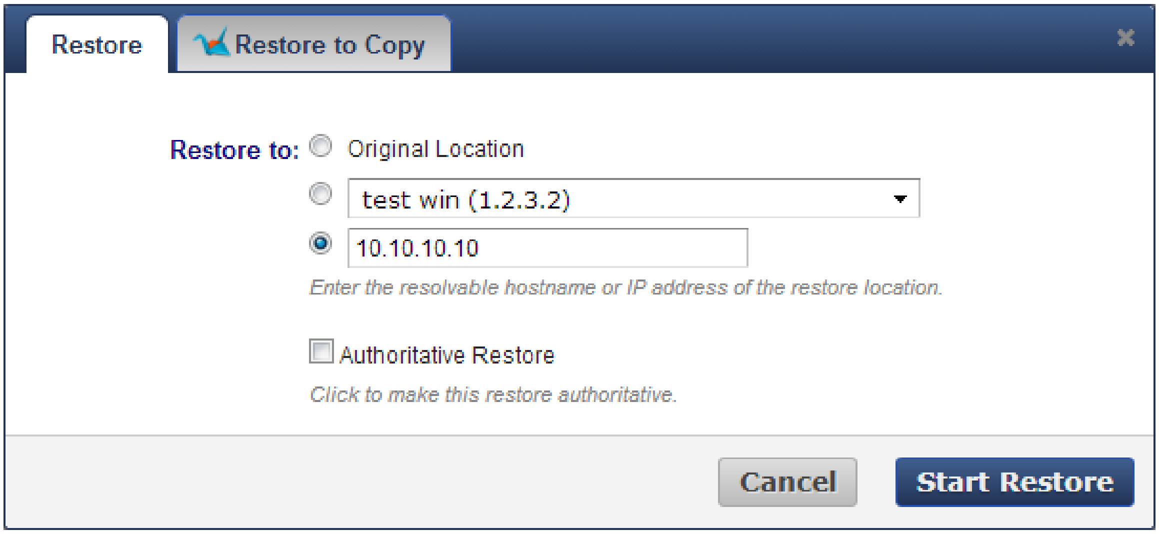
> ⚠ **Authoritative Restore**
> An authoritative restore returns the source server to the state it was in at the time of the backup, overwriting all changes made since that backup was performed. Changes made subsequent to that backup will be lost. For more information on authoritative restore, refer to the Microsoft TechNet article Active Directory Backup and Restore .

If the *target* server is set up with the same IP address as the *source* server you are restoring, select **Original Location**:



Restore to: ● Original Location
○ VMQA-OES2X64 (10.2.73.116)
○ Other Hostname or IP Address
Enter the resolvable hostname or IP address of the restore location.
☐ Authoritative Restore
Click to make this restore authoritative.

If the *target* server has a different IP address, select the third option and enter the IP address of the new location:



Restore to: ○ Original Location
○ test win (1.2.3.2)
● 10.10.10.10
Enter the resolvable hostname or IP address of the restore location.
☐ Authoritative Restore
Click to make this restore authoritative.

6. Click **Start Restore**.
7. Go to **REPORTS > Restore** to view restore job details.

> **Restore Job**
> The restore job completion time is dependent upon the size of the original server.

8. Once the restore is complete, a dialog displays. Click **OK** to close the dialog box.
9. Once the restore job is complete, use the steps in the section **Restoring Normal Boot Mode** to restore the server to normal mode.

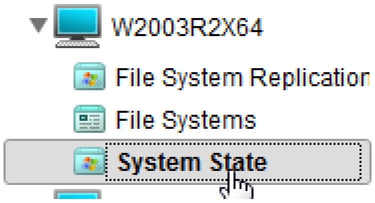
Restore System State

Use the procedure described in this section *only* if you wish to restore System State to the *target* server *without* restoring the rest of the file system as it was on the *source* server. This procedure restores System files including those in the **C:\Windows** folder. Perform the steps in this section if you are *not* performing full disaster recovery and wish to keep the *target* server's file system intact. Since this procedure does not restore file systems, following these steps will not restore replicated file systems or administration tools if the *source* server was a domain controller. This means group policy objects and log on scripts will not be available on the *target* server unless they are already on that server or on another server on the network. If you wish to restore file systems, use the steps described in the section **Restoring File System and System State**, or restore file systems manually from another server on the network.

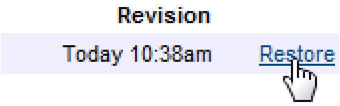
> Restoring System State from a *source* domain controller restores AD to its original state on that server; check with your system administrator before restoring a domain controller from an old revision backup.

To restore System State only,

1. Log in to the Barracuda Backup web interface, and go to **RESTORE > Restore Browser**.
2. Expand the Windows Server that represents the *source* server, and select **System State**:


W2003R2X64
File System Replication
File Systems
System State

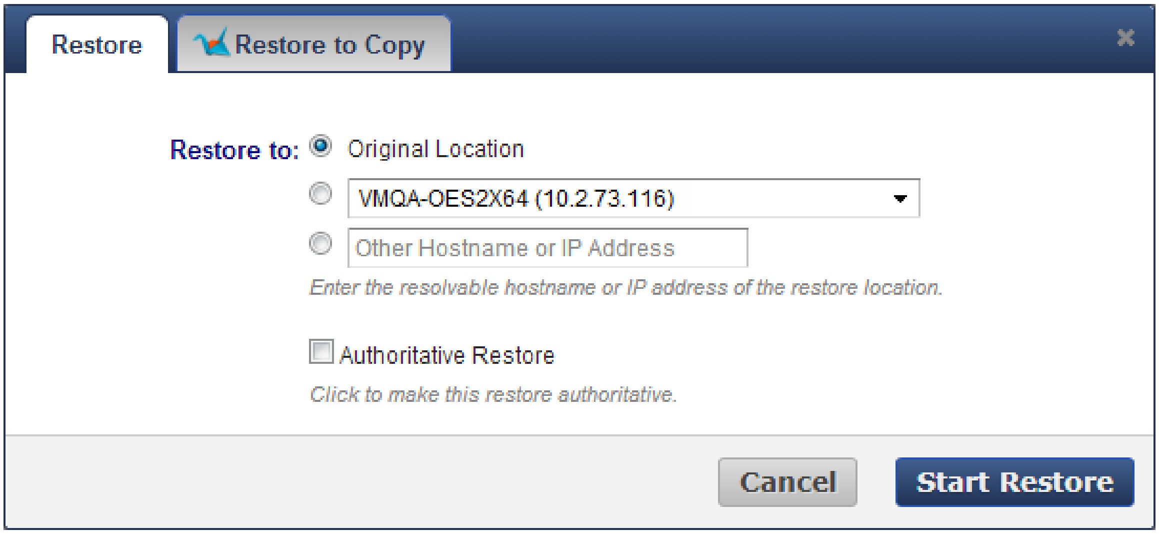
3. Click **View all revisions up to: <date>**; a list of revisions displays.
4. Click **Restore** next to the revision you wish to restore:


Revision
Today 10:38am
Restore

5. The **Restore** window displays.

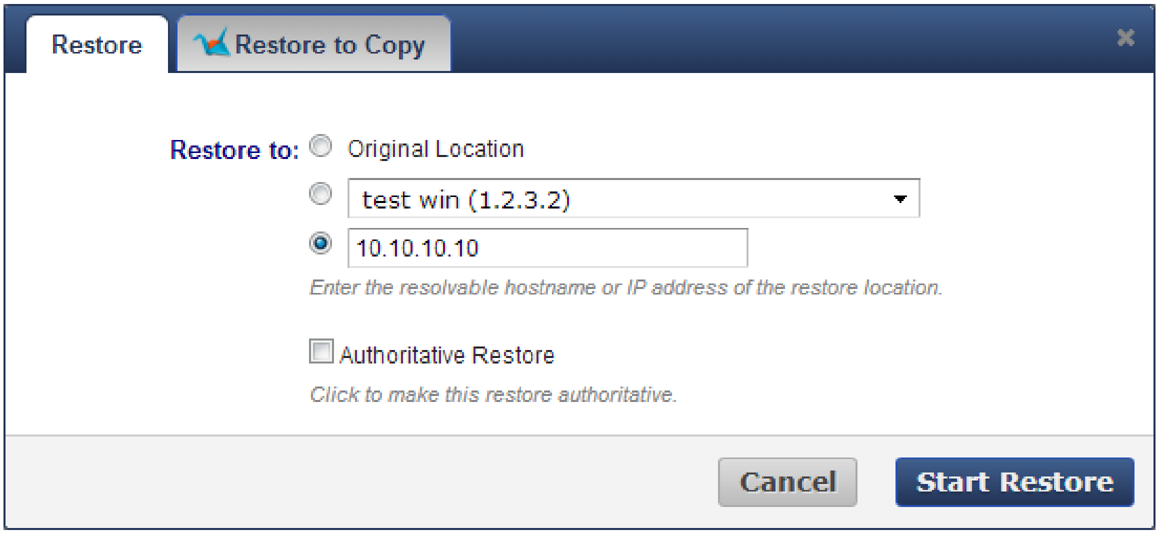
> **Authoritative Restore**
> An authoritative restore returns the source server to the state it was in at the time of the backup, overwriting all changes made since that backup was performed. Changes made subsequent to that backup will be lost. For more information on authoritative restore, refer to the Microsoft TechNet article Active Directory Backup and Restore .

If the *target* server is set up with the same IP address as the *source* server you are restoring, select **Original Location** :


Restore
Restore to Copy
Enter the resolvable hostname or IP address of the restore location.
Click to make this restore authoritative.
Cancel
Start Restore

Restore to: ● Original Location
○ VMQA-OES2X64 (10.2.73.116)
○ Other Hostname or IP Address
☐ Authoritative Restore

If the *target* server has a different IP address, select the third option and enter the IP address of the new location:


Restore
Restore to Copy
Enter the resolvable hostname or IP address of the restore location.
Click to make this restore authoritative.
Cancel
Start Restore

Restore to: ○ Original Location
○ test win (1.2.3.2)
● 10.10.10.10
☐ Authoritative Restore

6. Click **Start Restore** .
7. Go to **REPORTS > Restore** to view restore job details.

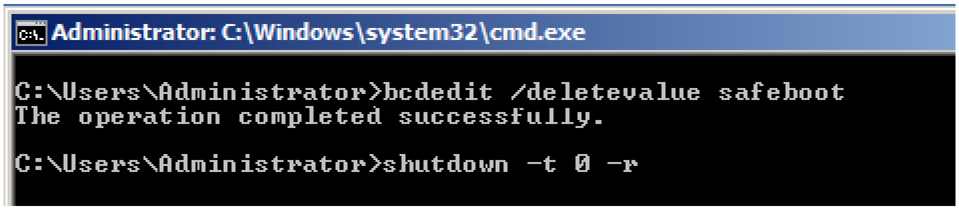
> **Restore Job**
> The restore job completion is dependent upon the size of the original server.

8. Once the restore is complete, a dialog displays. Click **OK** to close the dialog box.
9. Once the restore job is complete, use the steps in the section **Restoring Normal Boot Mode** to restore the server to normal mode.

Restore Normal Boot Mode

Once the restore is complete, use the following steps to restore the server to normal boot mode:

1. Power on the *target* server, or if it is already running, reboot the *target* server.
2. Log on using an administrator account; if the *target* server is a domain controller, log in using a domain account with administrative access to the server.
3. At a command prompt, enter the following command:
   ```
   bcdedit /deletevalue safeboot
   ```
4. Press **Enter**, and then enter the following command to restore normal boot mode:
   ```
   shutdown -t 0 -r
   ```



```
C:\Users\Administrator>bcdedit /deletevalue safeboot
The operation completed successfully.

C:\Users\Administrator>shutdown -t 0 -r
```

5. Press **Enter** to restart the server in normal boot mode.

How to Restore Exchange and GroupWise Messages

Related Articles
- Set Up GroupWise Message-Level Backups

Use the Barracuda Backup web interface to view, search, and restore Microsoft® Exchange and Novell® GroupWise messages. You can view all of the messages within a single mailbox, or select multiple mailboxes in which to search for a text string.

Use the following steps to restore messages using the Restore Browser:

1. Log in to the Barracuda Backup web interface, and in the left pane, click on the Barracuda Backup Server from which to restore data.
2. Go to the **RESTORE > Restore Browser** page, select the computer and the associated data source that contains the messages that you want to restore, and follow the on-screen instructions.

How to Restore a Windows System to Bare Metal

This article applies to Barracuda Backup Server firmware version 5.3 and higher.

"Bare metal" recovery allows you to restore a complete Microsoft® Windows system, including data, settings, applications, and operating system, onto a new computer on which nothing is installed.

Caution

The bare metal recovery process overwrites all existing data on the system to which you are restoring the data; therefore, bare metal recovery is recommended *only when no other recovery option is available.* This process rebuilds the target computer or server to its original system set up.

A bare metal restore is intended to be used for restoring to similar hardware.

All system volumes and system state must be backed up in order for bare metal recovery to be possible.

Requirements

You must have an existing backup of a system that uses one of the following Microsoft operating systems:

- Microsoft Windows Server 2012

- Microsoft Windows Server 2008 R2
- Windows 2008 Server
- Windows Small Business Server (SBS) 2011
- Windows SBS 2008
- Windows Vista
- Windows 8
- Windows 7

Additionally, you must have all of the following:

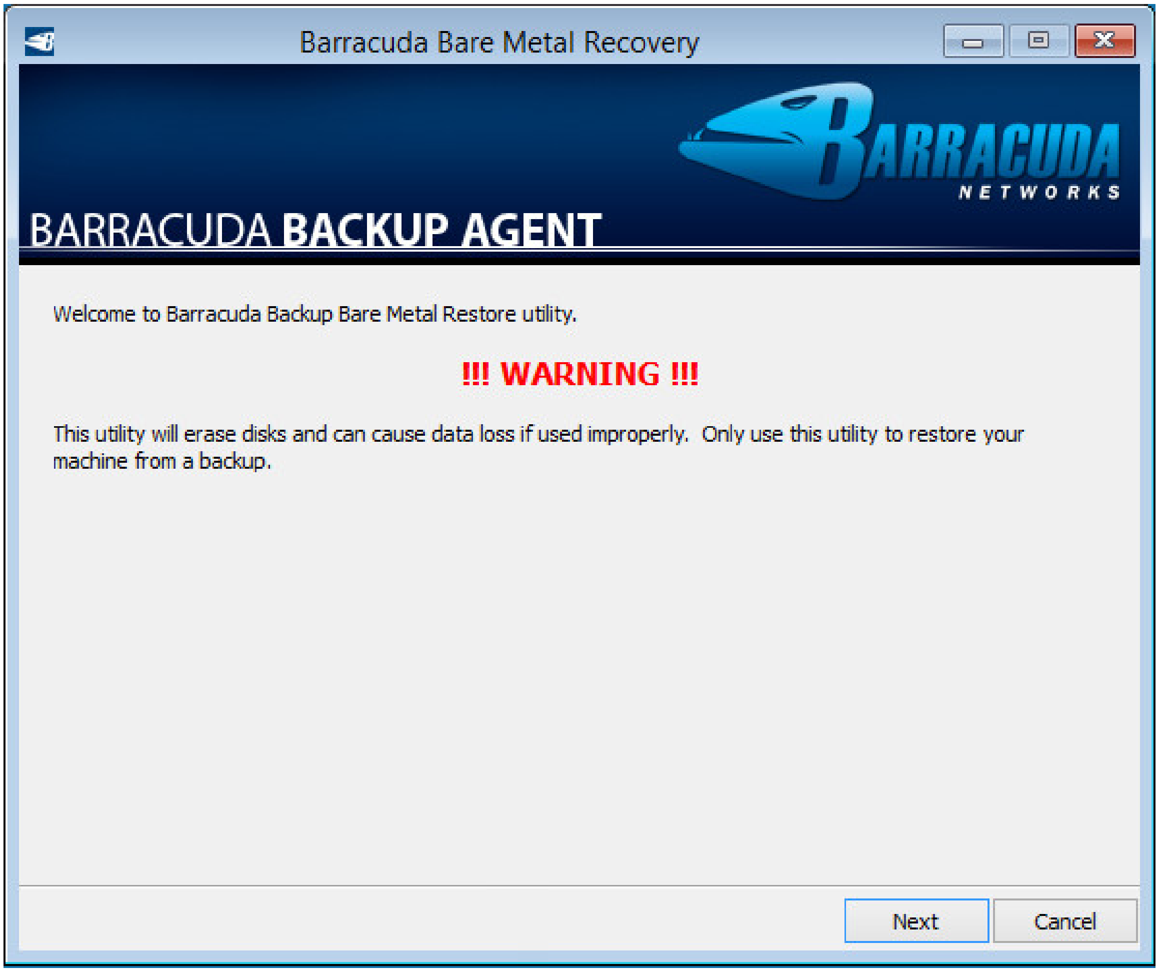
- Barracuda Backup Server firmware version 5.3 or higher;
- Barracuda Backup Bare Metal Live CD 5.3 or higher (available from the **SYSTEM > Software Downloads** page); and
- Administrator rights to the Microsoft Exchange Server.

Bare Metal Live CD

Use the following steps to download the Bare Metal Live CD boot media; select the appropriate bit version for the OS you are planning to restore. For example, if you are restoring a 64-bit operating system, you must use the 64-bit version.

1. Log in to Barracuda Backup and go to **SYSTEM > Software Downloads**. Download the Bare Metal Live ISO file to your local system.

2. Burn the Bare Metal Live ISO file to a CD.
3. Boot the system you want to restore using the Bare Metal Live CD you created in step 2.
4. Read the onscreen *warning:*


Barracuda Bare Metal Recovery
BARRACUDA NETWORKS
BARRACUDA BACKUP AGENT
Next
Cancel

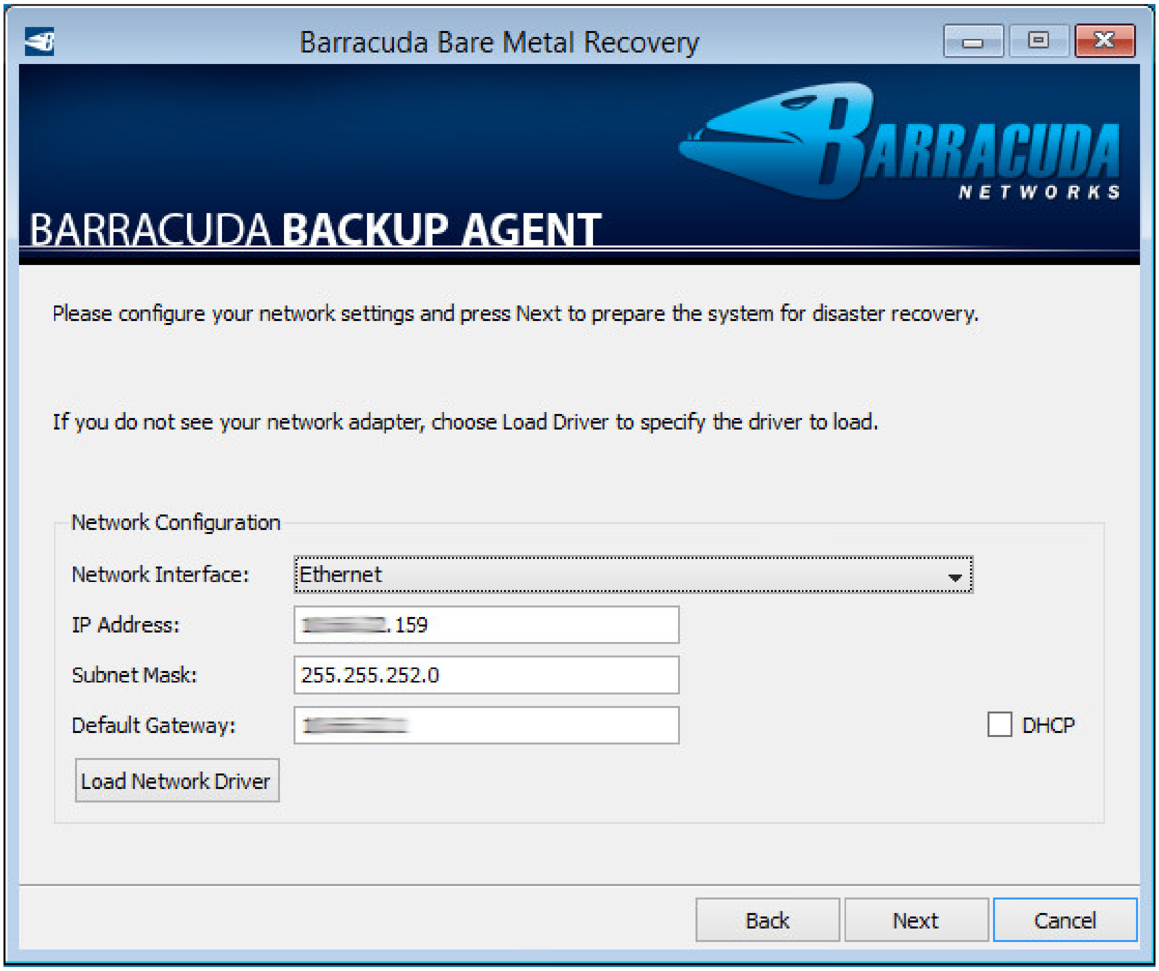
Welcome to Barracuda Backup Bare Metal Restore utility.

!!! WARNING !!!

This utility will erase disks and can cause data loss if used improperly. Only use this utility to restore your machine from a backup.

5. **To** continue with the Bare Metal restore, click **Next**.
6. Set up the **Network configuration**:

- If you have DHCP enabled on your network, an assigned IP address displays in the **IP Address** field.
- If DHCP is not enabled, uncheck **DHCP**, and enter the **IP Address**, **Subnet Mask**, and **Default Gateway**:


Barracuda Bare Metal Recovery
BARRACUDA NETWORKS
BARRACUDA BACKUP AGENT
Load Network Driver
Back
Next
Cancel

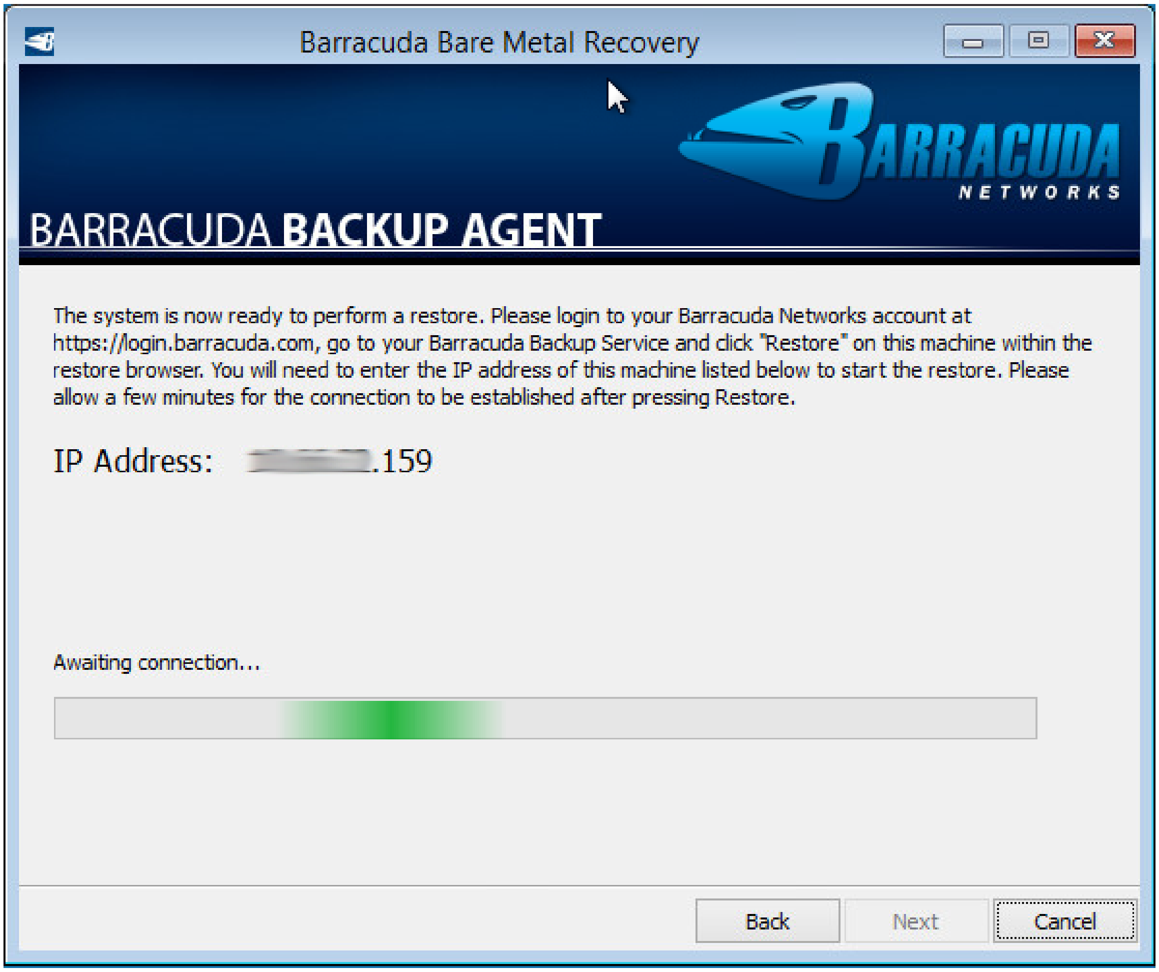
Please configure your network settings and press Next to prepare the system for disaster recovery.

If you do not see your network adapter, choose Load Driver to specify the driver to load.

Network Configuration

Network Interface: Ethernet
IP Address: [redacted].159
Subnet Mask: 255.255.252.0
Default Gateway: [redacted]
☐ DHCP

7. Click **Next**. You are prompted to log in to Barracuda Backup:

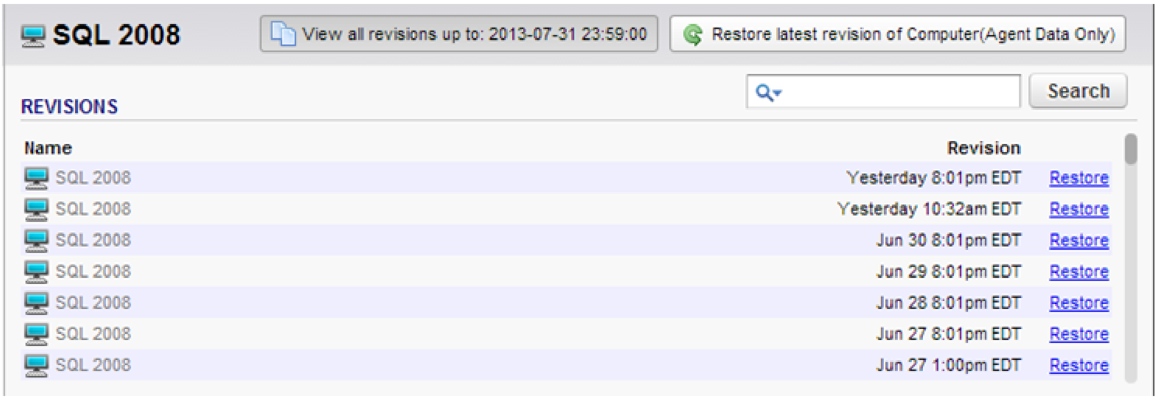

Barracuda Bare Metal Recovery
BARRACUDA NETWORKS
BARRACUDA BACKUP AGENT
Back
Next
Cancel

The system is now ready to perform a restore. Please login to your Barracuda Networks account at https://login.barracuda.com, go to your Barracuda Backup Service and click "Restore" on this machine within the restore browser. You will need to enter the IP address of this machine listed below to start the restore. Please allow a few minutes for the connection to be established after pressing Restore.

IP Address: [redacted].159

Awaiting connection...

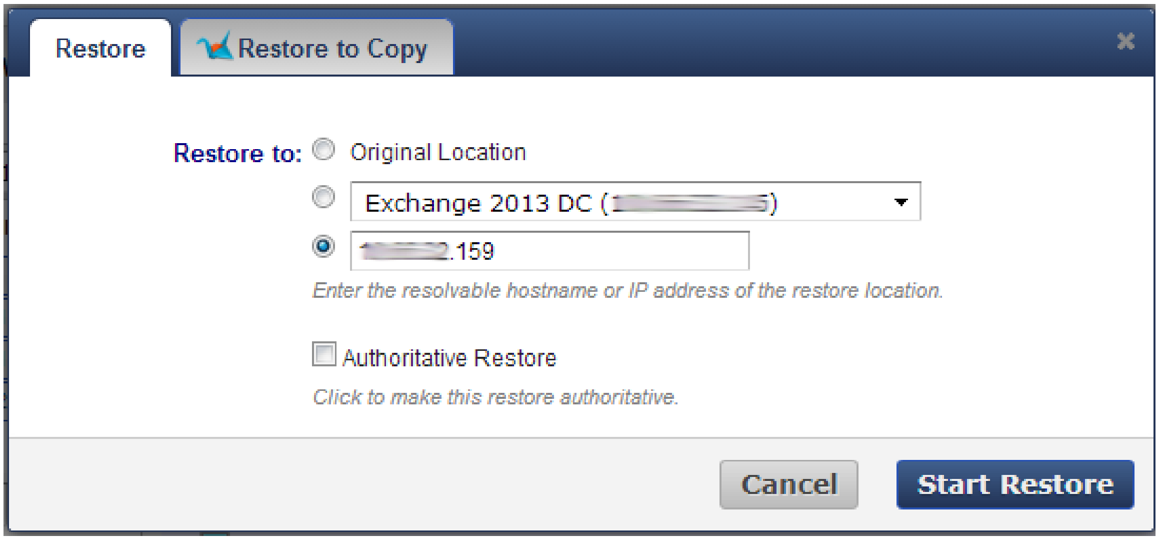
8. In the Barracuda Backup web interface, go to the **RESTORE > Restore Browser** page and select the system you want to recover.
9. Click **View all revisions up to: *<date>*** to view the selected system's revisions available for restore:


SQL 2008
View all revisions up to: 2013-07-31 23:59:00
Restore latest revision of Computer(Agent Data Only)
Search
REVISIONS

Name	Revision	
SQL 2008	Yesterday 8:01pm EDT	Restore
SQL 2008	Yesterday 10:32am EDT	Restore
SQL 2008	Jun 30 8:01pm EDT	Restore
SQL 2008	Jun 29 8:01pm EDT	Restore
SQL 2008	Jun 28 8:01pm EDT	Restore
SQL 2008	Jun 27 8:01pm EDT	Restore
SQL 2008	Jun 27 1:00pm EDT	Restore

10. In the **Revisions** list, click **Restore** for the revision you want to recover.

11. In the **Restore** dialog box, click the **Restore** tab, and enter the IP address of the system you are recovering in the **Restore to** section:


Restore
Restore to Copy
Cancel
Start Restore

Restore to: ○ Original Location

○ Exchange 2013 DC ([redacted])

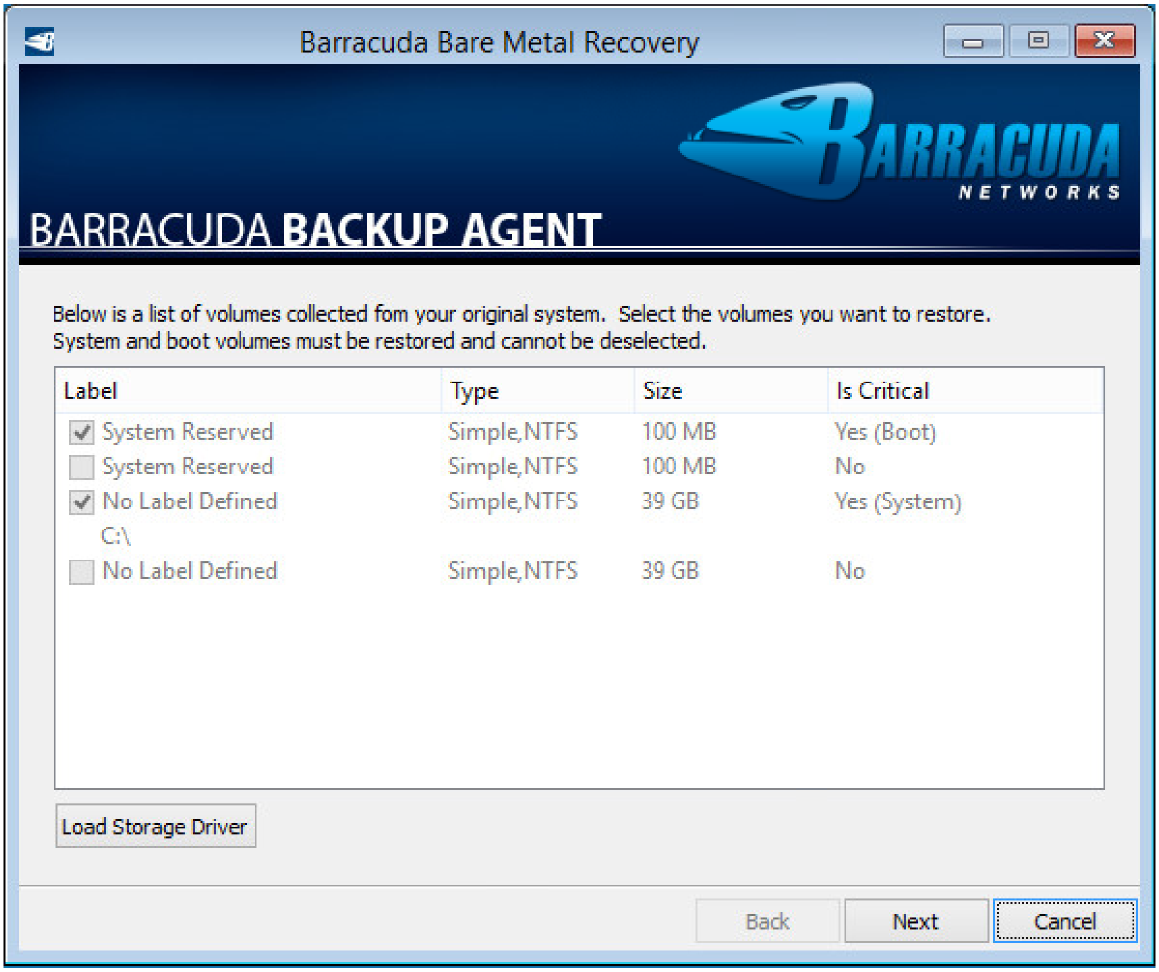
● [redacted].159

Enter the resolvable hostname or IP address of the restore location.

☐ Authoritative Restore

Click to make this restore authoritative.

12. Click **Start Restore**.
13. For the system booted using the Bare Metal Live CD, a list of volumes that are recoverable displays:


Barracuda Bare Metal Recovery
BARRACUDA
NETWORKS
BARRACUDA BACKUP AGENT
Load Storage Driver
Back
Next
Cancel

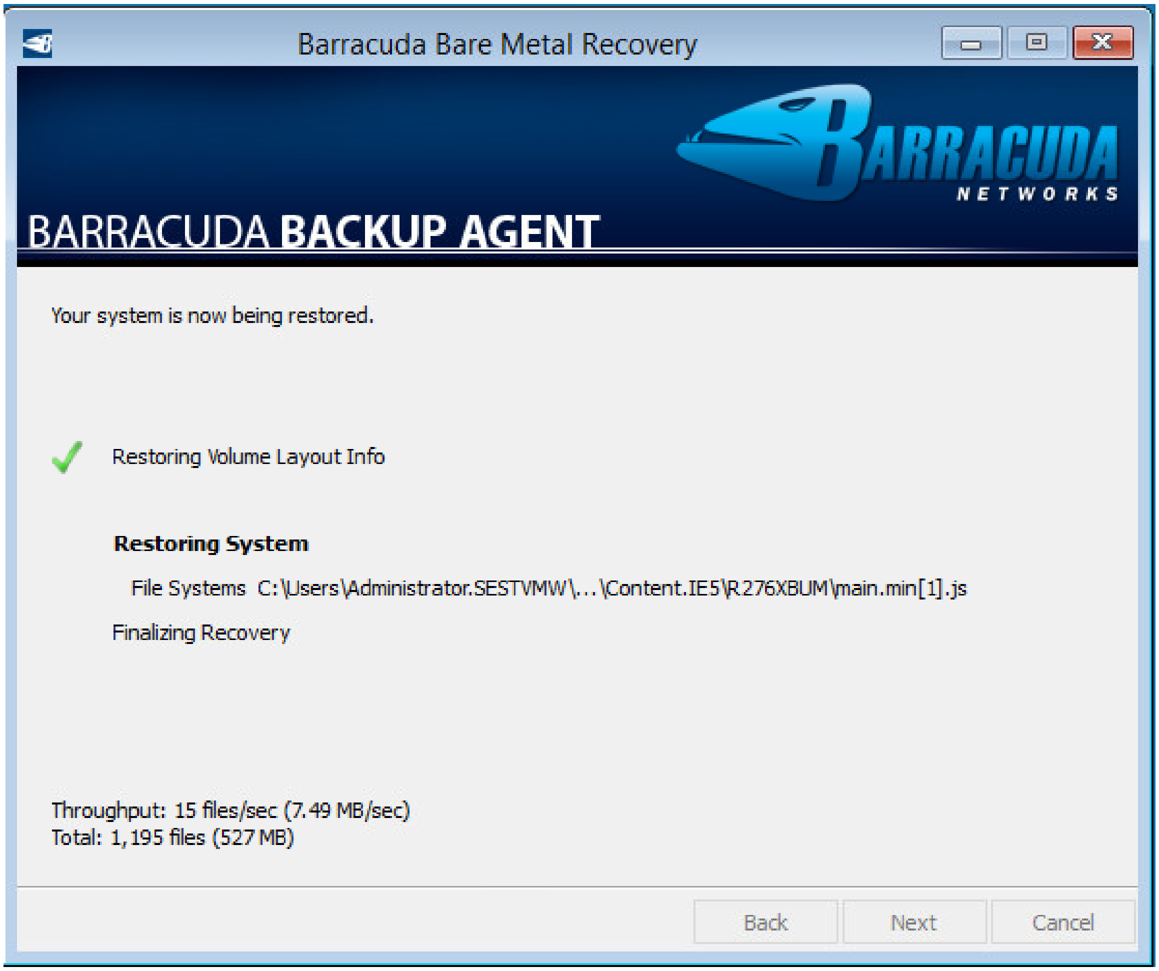
Below is a list of volumes collected fom your original system. Select the volumes you want to restore.
System and boot volumes must be restored and cannot be deselected.

Label	Type	Size	Is Critical
☑ System Reserved	Simple,NTFS	100 MB	Yes (Boot)
☐ System Reserved	Simple,NTFS	100 MB	No
☑ No Label Defined C:\	Simple,NTFS	39 GB	Yes (System)
☐ No Label Defined	Simple,NTFS	39 GB	No

14. Select the volumes you want to recover.

> **Boot and System Volumes**
> You cannot deselect boot and system volumes as these are required for the Bare Metal restore.

15. Click **Next** to begin the restore:



Barracuda Bare Metal Recovery
BARRACUDA NETWORKS
BARRACUDA BACKUP AGENT
Back
Next
Cancel

Your system is now being restored.

✓ Restoring Volume Layout Info

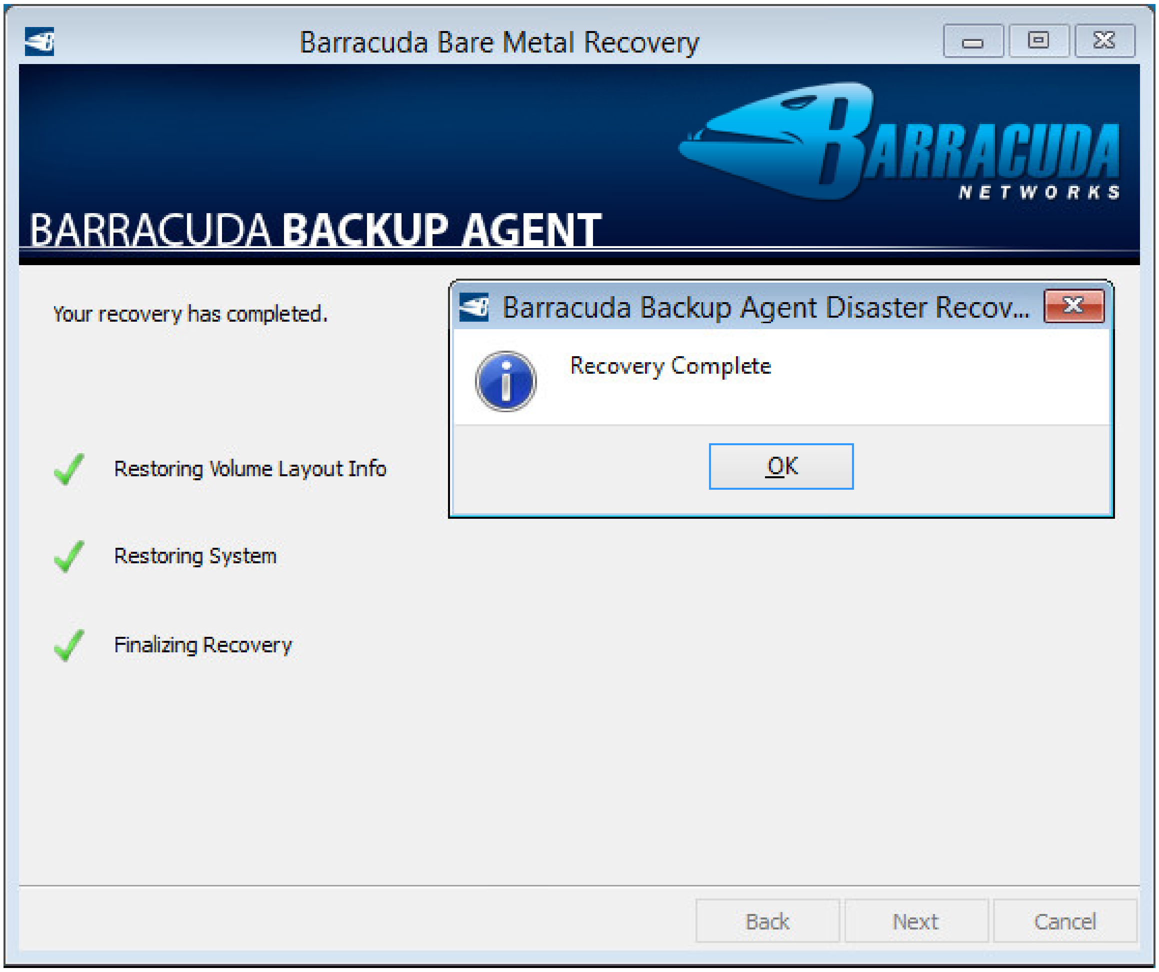
Restoring System

File Systems C:\Users\Administrator.SESTVMW\...\Content.IE5\R276XBUM\main.min[1].js

Finalizing Recovery

Throughput: 15 files/sec (7.49 MB/sec)
Total: 1,195 files (527 MB)

16. When the restore is complete, click **OK** in the **Confirmation** dialog box:


Barracuda Bare Metal Recovery
BARRACUDA NETWORKS
BARRACUDA BACKUP AGENT
Barracuda Backup Agent Disaster Recov...
OK
Back
Next
Cancel

Your recovery has completed.

✓ Restoring Volume Layout Info

✓ Restoring System

✓ Finalizing Recovery

Recovery Complete

17. Remove the bare Metal Live CD, and reboot the system.

> **SQL and Exchange Server**
> If SQL and/or Exchange are installed on the system, you are required to restore those items separately once the bare metal restore is complete.

How to Restore a Linux Server Using Bare Metal Restore

This article refers to firmware version 5.3 and higher, and the Barracuda Linux Backup Agent 5.3 and higher.

In this article:

- Step 1. Install the Barracuda Linux Backup Agent
- Step 2. Partition, Format, and Create the File System
- Step 3. Restore the File System Using the Barracuda Linux Backup Agent
- Step 4. Mount the Linux System Directories and Install a Bootloader

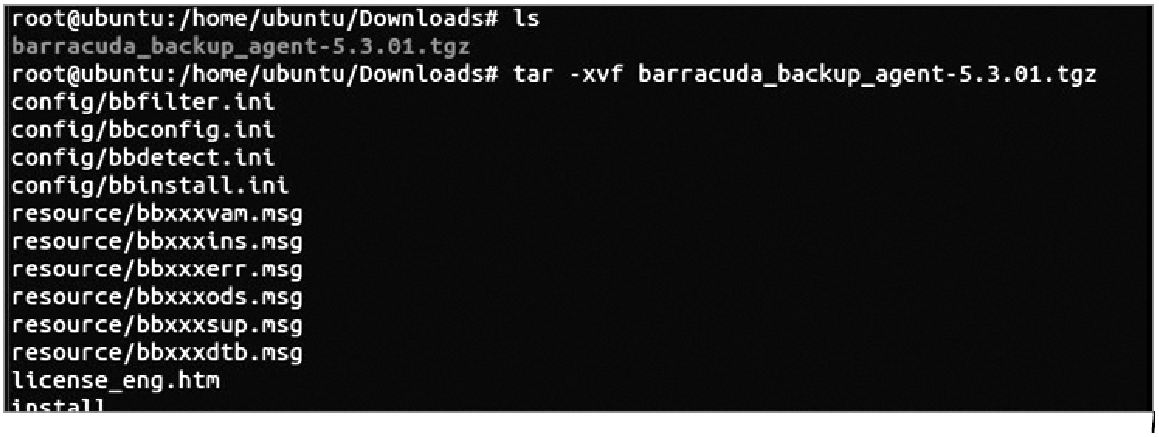
> Linux distributions (distros) that support Live CDs can *only* be restored to bare metal; for example, Red Hat, Fedora, Ubuntu, Gentoo, and SUSE Linux.

Use the following steps to restore an entire file system backed up using the Barracuda Linux Backup Agent.

> **Example**
> The following steps are based on Ubuntu Desktop 12.04 x64.

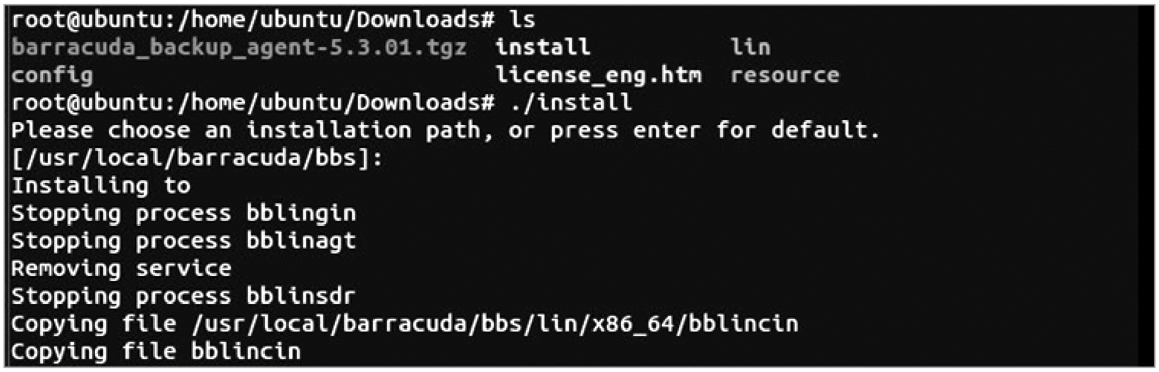
Step 1. Install the Barracuda Linux Backup Agent

1. Boot into a live CD environment that supports your hardware, for example, Ubuntu 12.04 x64.
2. Configure an IP address, and verify network connectivity to the Barracuda Backup Server containing the data source files you want to restore.
3. In the Barracuda Backup web interface, go to the **SYSTEM > Software Downloads** page.
4. Download and unzip the Barracuda Linux Backup Agent to your live booted environment.
5. Unpack the tar file:
   `tar -xvf barracuda_backup_agent-x.x.x.tgz`
   For example:



```
root@ubuntu:/home/ubuntu/Downloads# ls
barracuda_backup_agent-5.3.01.tgz
root@ubuntu:/home/ubuntu/Downloads# tar -xvf barracuda_backup_agent-5.3.01.tgz
config/bbfilter.ini
config/bbconfig.ini
config/bbdetect.ini
config/bbinstall.ini
resource/bbxxxvam.msg
resource/bbxxxins.msg
resource/bbxxxerr.msg
resource/bbxxxods.msg
resource/bbxxxsup.msg
resource/bbxxxdtb.msg
license_eng.htm
install
```

6. On the live booted environment, and change the directory to the Barracuda Linux Backup Agent directory, for example:
   `/Desktop/agent-5.3-lin$`
7. Install the agent:
   `./install`
   For example:

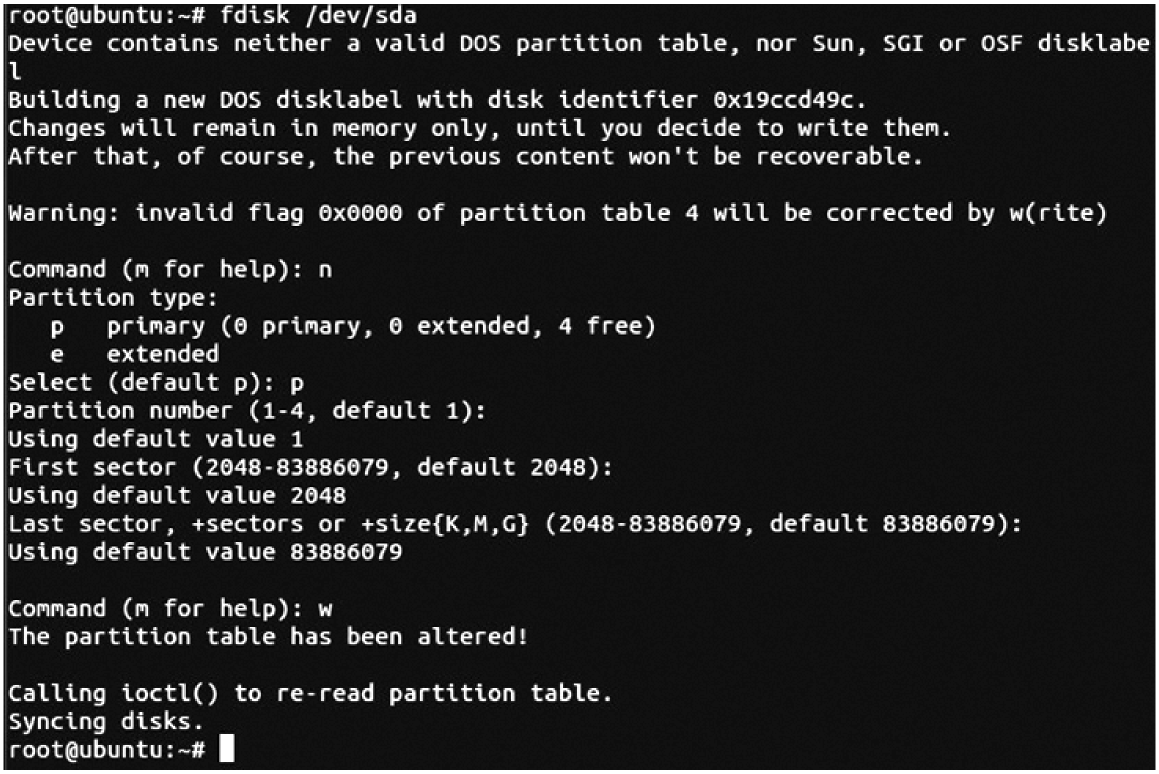


```
root@ubuntu:/home/ubuntu/Downloads# ls
barracuda_backup_agent-5.3.01.tgz  install          lin
config                             license_eng.htm  resource
root@ubuntu:/home/ubuntu/Downloads# ./install
Please choose an installation path, or press enter for default.
[/usr/local/barracuda/bbs]:
Installing to
Stopping process bblingin
Stopping process bblinagt
Removing service
Stopping process bblinsdr
Copying file /usr/local/barracuda/bbs/lin/x86_64/bblincin
Copying file bblincin
```

Step 2. Partition, Format, and Create the File System

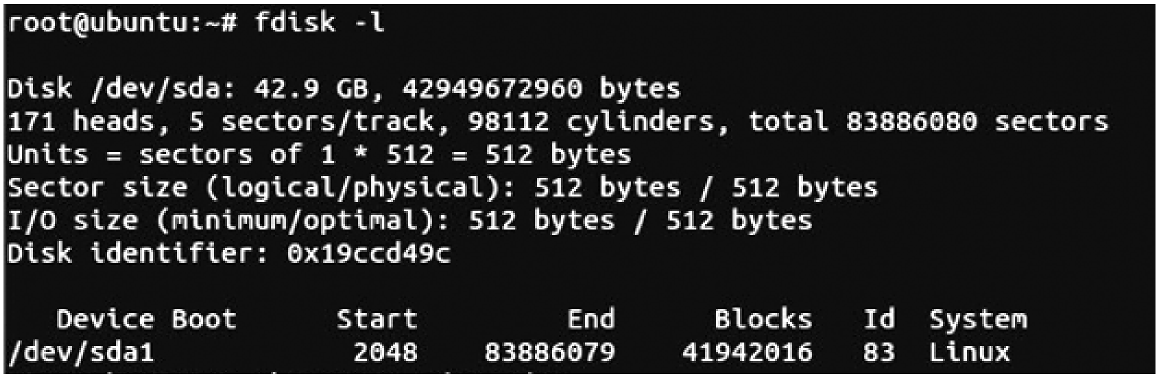
> The destination file system(s) must be empty. If you have multiple mount points, you must mount them such that the backup paths match during restore. For example, if you have a separate root and home partition, mount the root partition at **/mnt/system** and the home partition at **/mnt/system/home**. Configure the restore to target the path **/mnt/system/**.

1. Open a terminal window, and enter the following command to create the partition:
   `fdisk /dev/sda`
2. Press **Return**. Enter `N` to create a new partition, and press **Return**.
3. Enter `P` the primary partition, and press **Return**.
4. Enter the partition number, for example, enter `1` for partition 1. Press **Return**.
5. Press **Enter** to select the default first sector, and then press **Enter** again to select teh default last sector.
6. Enter `W`, and press **Enter** to write the changes:



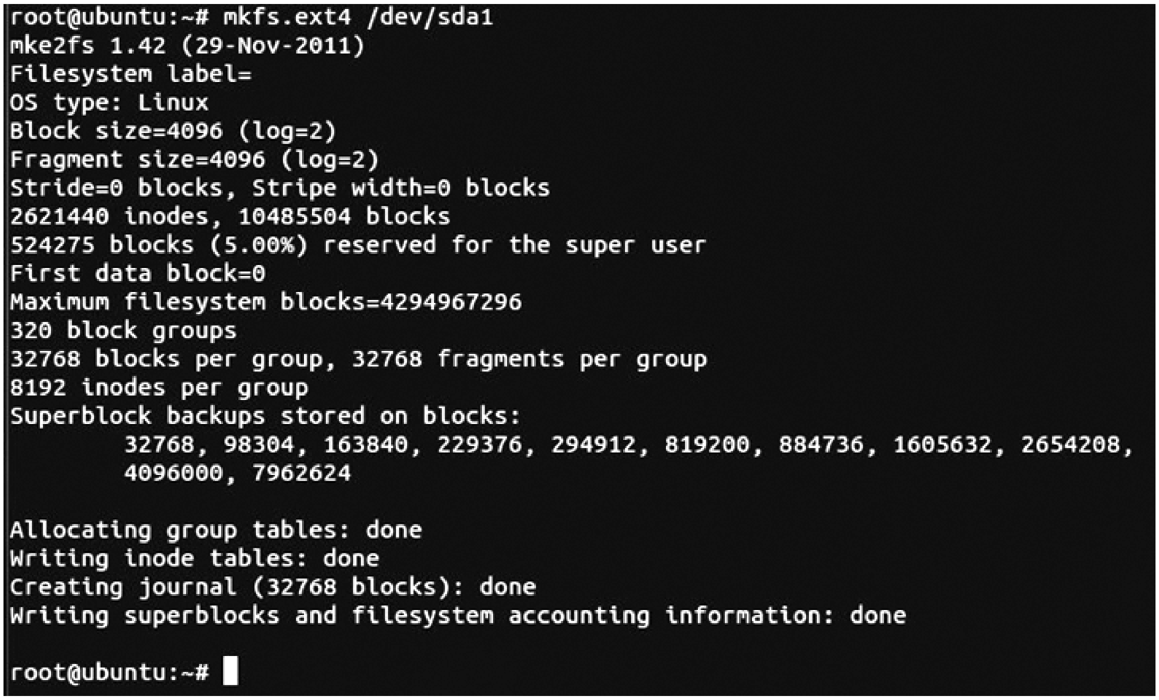
```
root@ubuntu:~# fdisk /dev/sda
Device contains neither a valid DOS partition table, nor Sun, SGI or OSF disklabe
l
Building a new DOS disklabel with disk identifier 0x19ccd49c.
Changes will remain in memory only, until you decide to write them.
After that, of course, the previous content won't be recoverable.

Warning: invalid flag 0x0000 of partition table 4 will be corrected by w(rite)

Command (m for help): n
Partition type:
   p   primary (0 primary, 0 extended, 4 free)
   e   extended
Select (default p): p
Partition number (1-4, default 1):
Using default value 1
First sector (2048-83886079, default 2048):
Using default value 2048
Last sector, +sectors or +size{K,M,G} (2048-83886079, default 83886079):
Using default value 83886079

Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.
Syncing disks.
root@ubuntu:~# 
```

7. Enter `fdisk -l` and press **Return** to view the partitions:



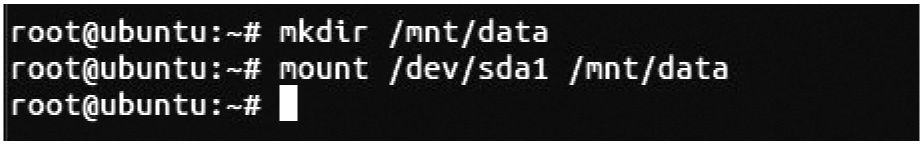
```
root@ubuntu:~# fdisk -l

Disk /dev/sda: 42.9 GB, 42949672960 bytes
171 heads, 5 sectors/track, 98112 cylinders, total 83886080 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x19ccd49c

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1            2048    83886079    41942016   83  Linux
```

8. Enter `mkfs.ext4 /dev/sda1` and press **Return** to create the file system:



```
root@ubuntu:~# mkfs.ext4 /dev/sda1
mke2fs 1.42 (29-Nov-2011)
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
2621440 inodes, 10485504 blocks
524275 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=4294967296
320 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
        4096000, 7962624

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done

root@ubuntu:~#
```

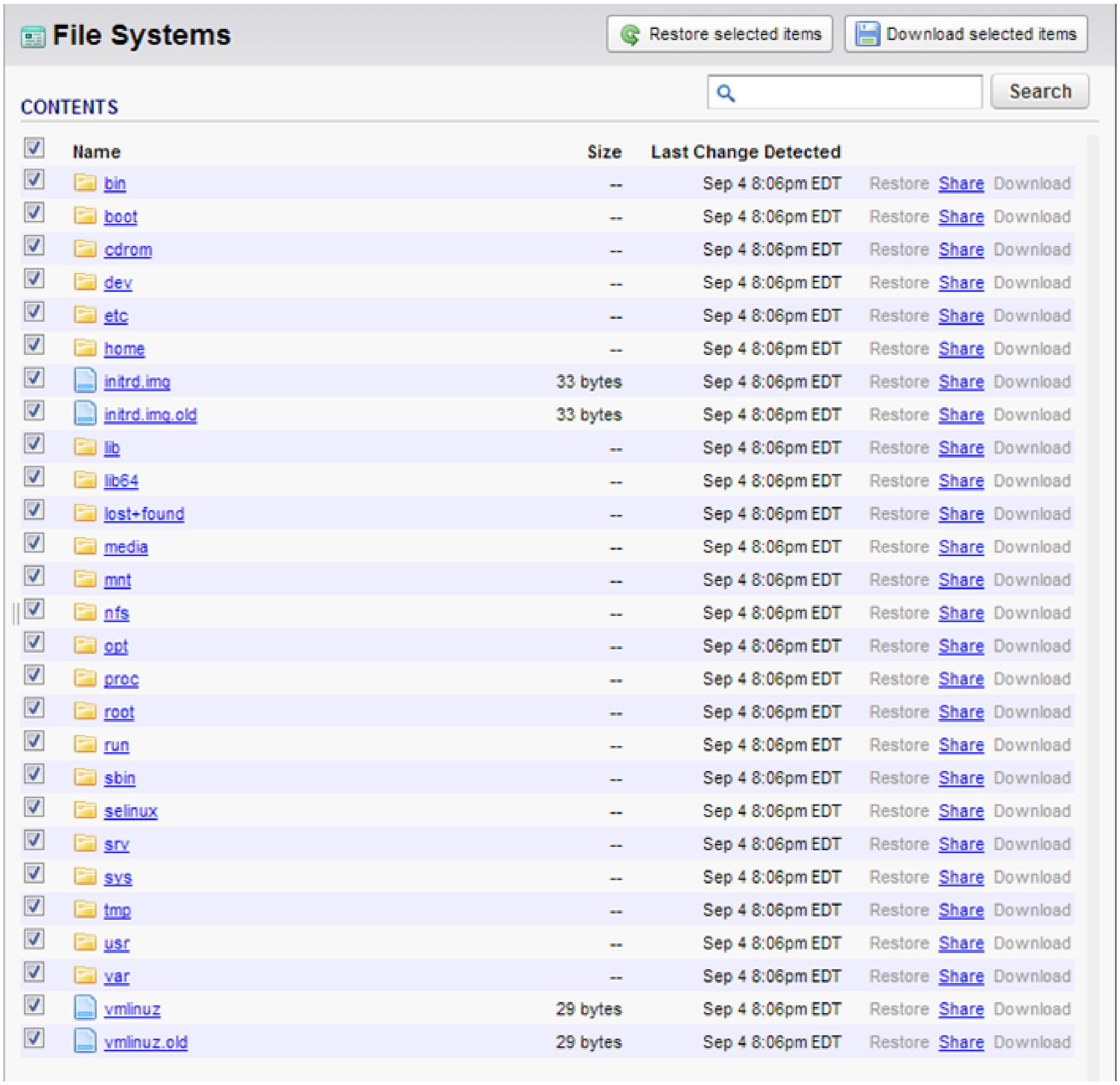
9. Enter the mount point, and press **Return**. For example:



```
root@ubuntu:~# mkdir /mnt/data
root@ubuntu:~# mount /dev/sda1 /mnt/data
root@ubuntu:~#
```

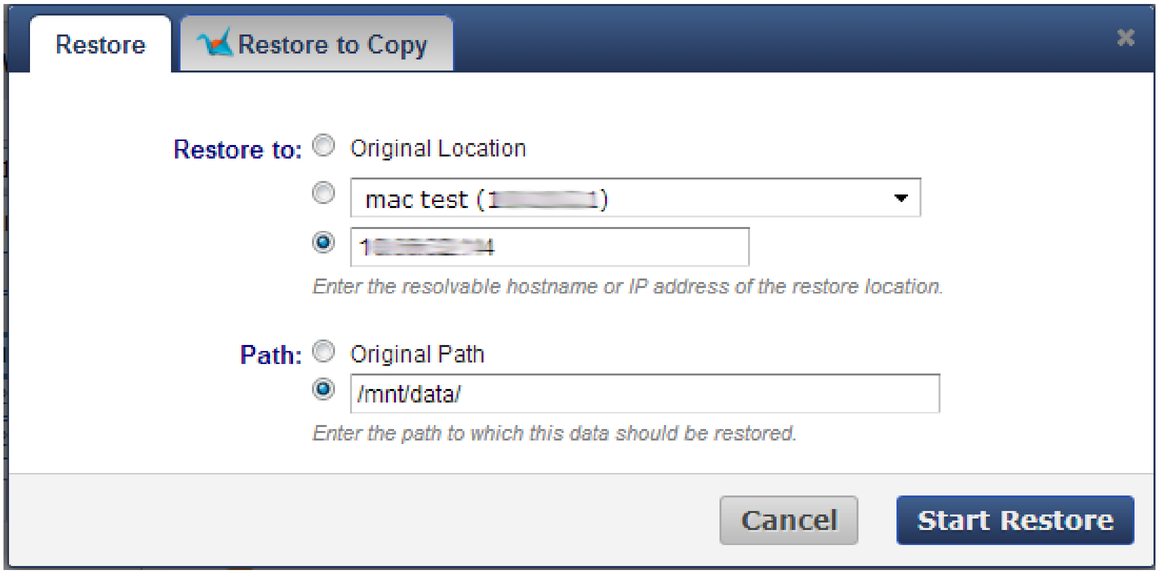
Step 3. Restore the File System Using the Barracuda Linux Backup Agent

1. Log in to the Barracuda Backup Server, and go to **RESTORE > Restore Browser** page.
2. Select and expand the Linux Server you wish to restore; select **File Systems**.
3. In the right pane, click the top check box to select all contents:



☑	Name	Size	Last Change Detected			
☑	bin	--	Sep 4 8:06pm EDT	Restore	Share	Download
☑	boot	--	Sep 4 8:06pm EDT	Restore	Share	Download
☑	cdrom	--	Sep 4 8:06pm EDT	Restore	Share	Download
☑	dev	--	Sep 4 8:06pm EDT	Restore	Share	Download
☑	etc	--	Sep 4 8:06pm EDT	Restore	Share	Download
☑	home	--	Sep 4 8:06pm EDT	Restore	Share	Download
☑	initrd.img	33 bytes	Sep 4 8:06pm EDT	Restore	Share	Download
☑	initrd.img.old	33 bytes	Sep 4 8:06pm EDT	Restore	Share	Download
☑	lib	--	Sep 4 8:06pm EDT	Restore	Share	Download
☑	lib64	--	Sep 4 8:06pm EDT	Restore	Share	Download
☑	lost+found	--	Sep 4 8:06pm EDT	Restore	Share	Download
☑	media	--	Sep 4 8:06pm EDT	Restore	Share	Download
☑	mnt	--	Sep 4 8:06pm EDT	Restore	Share	Download
☑	nfs	--	Sep 4 8:06pm EDT	Restore	Share	Download
☑	opt	--	Sep 4 8:06pm EDT	Restore	Share	Download
☑	proc	--	Sep 4 8:06pm EDT	Restore	Share	Download
☑	root	--	Sep 4 8:06pm EDT	Restore	Share	Download
☑	run	--	Sep 4 8:06pm EDT	Restore	Share	Download
☑	sbin	--	Sep 4 8:06pm EDT	Restore	Share	Download
☑	selinux	--	Sep 4 8:06pm EDT	Restore	Share	Download
☑	srv	--	Sep 4 8:06pm EDT	Restore	Share	Download
☑	sys	--	Sep 4 8:06pm EDT	Restore	Share	Download
☑	tmp	--	Sep 4 8:06pm EDT	Restore	Share	Download
☑	usr	--	Sep 4 8:06pm EDT	Restore	Share	Download
☑	var	--	Sep 4 8:06pm EDT	Restore	Share	Download
☑	vmlinuz	29 bytes	Sep 4 8:06pm EDT	Restore	Share	Download
☑	vmlinuz.old	29 bytes	Sep 4 8:06pm EDT	Restore	Share	Download

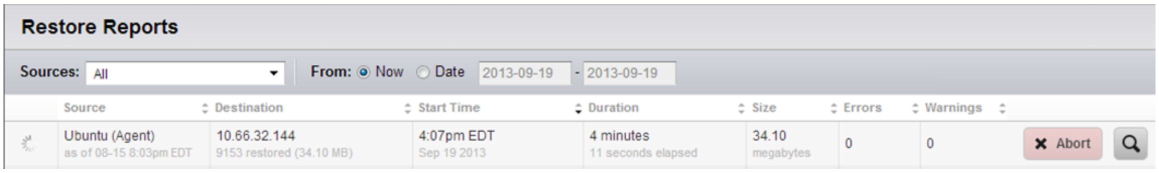
4. Click **Restore selected items** at the top of the screen.
5. In the **Restore** dialog, enter the target IP address of the live booted machine, and enter the mount point to which to restore, for example, **/mnt/data/**:



Restore to: ○ Original Location
○ mac test ([redacted])
● [redacted]
Enter the resolvable hostname or IP address of the restore location.

Path: ○ Original Path
● /mnt/data/
Enter the path to which this data should be restored.

6. Click **Start Restore**. To view the restore progress, go to the **Reports > Restore** page:

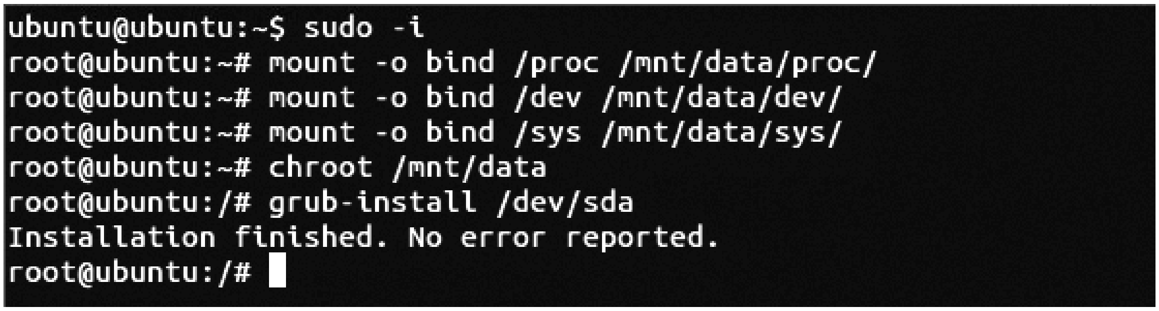


Source	Destination	Start Time	Duration	Size	Errors	Warnings
Ubuntu (Agent) as of 08-15 8:03pm EDT	10.66.32.144 9153 restored (34.10 MB)	4:07pm EDT Sep 19 2013	4 minutes 11 seconds elapsed	34.10 megabytes	0	0

Step 4. Mount the Linux System Directories and Install a Bootloader

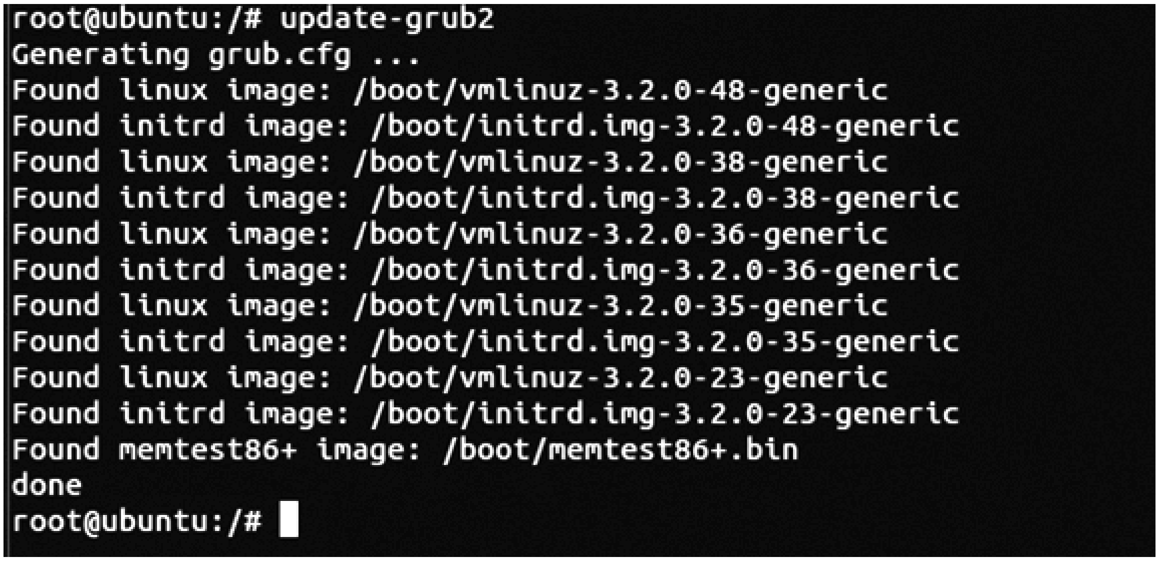
Complete the following steps when the restore is 100% complete and successful.

1. Open a terminal window, and enter the following commands to mount the Linux system directories and install a bootloader using your mount points:



```
ubuntu@ubuntu:~$ sudo -i
root@ubuntu:~# mount -o bind /proc /mnt/data/proc/
root@ubuntu:~# mount -o bind /dev /mnt/data/dev/
root@ubuntu:~# mount -o bind /sys /mnt/data/sys/
root@ubuntu:~# chroot /mnt/data
root@ubuntu:/# grub-install /dev/sda
Installation finished. No error reported.
root@ubuntu:/# 
```

2. Enter `update-grub2` and press **Return** to update the grub bootloader:



```
root@ubuntu:/# update-grub2
Generating grub.cfg ...
Found linux image: /boot/vmlinuz-3.2.0-48-generic
Found initrd image: /boot/initrd.img-3.2.0-48-generic
Found linux image: /boot/vmlinuz-3.2.0-38-generic
Found initrd image: /boot/initrd.img-3.2.0-38-generic
Found linux image: /boot/vmlinuz-3.2.0-36-generic
Found initrd image: /boot/initrd.img-3.2.0-36-generic
Found linux image: /boot/vmlinuz-3.2.0-35-generic
Found initrd image: /boot/initrd.img-3.2.0-35-generic
Found linux image: /boot/vmlinuz-3.2.0-23-generic
Found initrd image: /boot/initrd.img-3.2.0-23-generic
Found memtest86+ image: /boot/memtest86+.bin
done
root@ubuntu:/# 
```

3. Reboot the system.

How to Restore Data with FTPES

This article refers to Barracuda Backup firmware 4.2 and earlier *only*.

You can use FTPES to restore data if your local Barracuda Backup Server is not currently accessible, or if you are not on the same network as your local Barracuda Backup Server. This is not for data stored by the Barracuda Backup Agent. This option is used:

- For file share data only
- To restore data directly from Barracuda Cloud Storage

Programs such as FileZilla for Windows and Linux, and Transmit for Mac OS X, work well.

To use FTPES to restore data,

1. Download, install, and launch an FTPES client.
2. Connect to the server/host `restore.barracuda.com`.
3. Your account must have administrator rights to restore files. The username and password are the same as those used to access the Barracuda Backup web interface.
4. Select the **FTPES** protocol and standard port **21**.
5. Upon connection, a listing of directories displays. Follow the directory structure to the date when you would like to restore your data. Past those directories, the backed up servers display. After servers, you are presented with each share that you backed up on that server. Locate the data you want to restore.
6. Drag the data to restore from the connection to a location on your system. All of the data is retrieved from the Barracuda Cloud Storage.

Legacy Firmware Recovery and Restoration Options

In this Section

The following articles refer to recovery and restore options available *on firmware version 4.3 or earlier only*.

- How to Use Windows Explorer and WebDAV
- How to Restore Data with an FTP Client
- Barracuda Restore for Windows

How to Use Windows Explorer and WebDAV

This article refers to Barracuda Backup firmware 4.2 and earlier *only*.

The Barracuda Backup Server supports the web-based Distributed Authoring and Versioning (WebDAV) protocol, which defines how users can access and manage documents on a remote server. This option is used:

- For file share data only
- Only if you are on the same network as the local Barracuda Backup Server

Most Internet browsers have a WebDAV client. In the browser address bar, type `http://`*`Barracuda Backup Server IP Address`*`:8080` to connect directly to the local Barracuda Backup Server.

Windows users can restore data from the local Barracuda Backup Server using the built-in Windows Explorer as follows:

1. On a Windows system, go to **My Network Places**.
2. On the sidebar, click **Add Network Place** to start the wizard.
3. Select **Choose Another Network Location**, and then click **Next**.
4. Enter **http://*Barracuda Backup Server IP Address*:8080** and then click **Next**.
5. Your account must have administrator rights to restore files. The username and password are the same as those used to access the Barracuda Backup web interface.
6. Follow the instructions to finish the connection.
7. Once you are connected you are presented with a list of directories on the Barracuda Backup Server. The directories are labeled by year and include subdirectories for each month, and within each month there is a directory for each day. Each daily directory contains folders for the servers and directory shares that are deployed on the Barracuda Backup Server. The data files that can be restored are located within each server's directory share.
8. You can select and restore files by right clicking on them, or you can drag and drop files from the Barracuda Backup Server to a directory on your network or local system.

How to Restore Data with an FTP Client

This article refers to Barracuda Backup firmware 4.2 and earlier *only*.

An FTP client can be used to restore data securely and quickly. This is not for data stored by the Barracuda Backup Agent.

Related Articles
• How to Restore Data with FTPES

An FTP client is used for the following:

- Local restores of file share data only
- Only if you are on the same network as the local Barracuda Backup Server

Programs such as FileZilla for Windows and Linux, and Transmit for Mac OS X, work well.

To use FTP to restore data,

1. Download, install, and launch an FTP client.
2. Your account must have administrator rights to restore files. The username and password are the same as those used to access the Barracuda Backup web interface.
3. Enter the IP address of the local Barracuda Backup Server. Use **FTP protocol**, and standard port **21**.
4. Upon connection, a listing of directories displays. Past those directories, you are shown each server that is backed up by the Barracuda Backup Server. After servers, you are presented with each share that you backed up on that server. Now you can find the data you want to restore.
5. Drag the data to restore from the Barracuda Backup Server connection to a location on your system. The Barracuda Backup Server first attempts to retrieve its data locally. If some of your data is no longer local, it automatically fetches it from an offsite storage location.

Barracuda Restore for Windows

In this Section

ⓘ Use **Barracuda Restore for Windows** for Barracuda Backup firmware release 4.3 and earlier *only*.

- How to Set Up Barracuda Restore for Windows
- How to Customize Barracuda Restore for Windows
- How to Run Barracuda Restore for Windows
- How to Restore Data Using Barracuda Restore for Windows

How to Set Up Barracuda Restore for Windows

This article refers to Barracuda Backup firmware version 4.3 and earlier *only*.

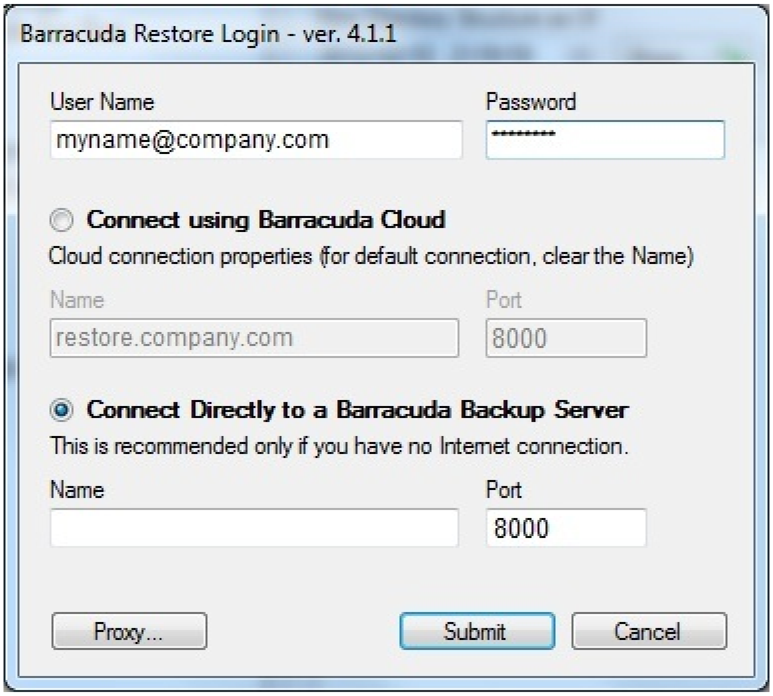
In this article:

- Install Barracuda Restore for Windows
- Set Up Restore Connections
- Log In
- View New Features List
- Modify Backup Server Location

Install Barracuda Restore for Windows

To install Barracuda Restore for Windows, log into the Barracuda Backup web interface, go to **SUPPORT > Software Downloads**, and click the **Download** link for the Barracuda Restore Tool. Save and run the installer to add Barracuda Restore for Windows® to your local system; note that you must have administrator rights on the system on which you are installing Barracuda Restore for Windows.
Set Up Restore Connections

To set up the restore connection, from the **Start** menu on your local system, go to **Barracuda > Barracuda Restore**; the **Login** window displays:


Barracuda Restore Login - ver. 4.1.1
User Name
Password
Connect using Barracuda Cloud
Cloud connection properties (for default connection, clear the Name)
Name
Port
Connect Directly to a Barracuda Backup Server
This is recommended only if you have no Internet connection.
Name
Port
Proxy...
Submit
Cancel

User Name: myname@company.com
Password: *********

○ Connect using Barracuda Cloud
Name: restore.company.com
Port: 8000

● Connect Directly to a Barracuda Backup Server
Name:
Port: 8000

To set up the restore connection,

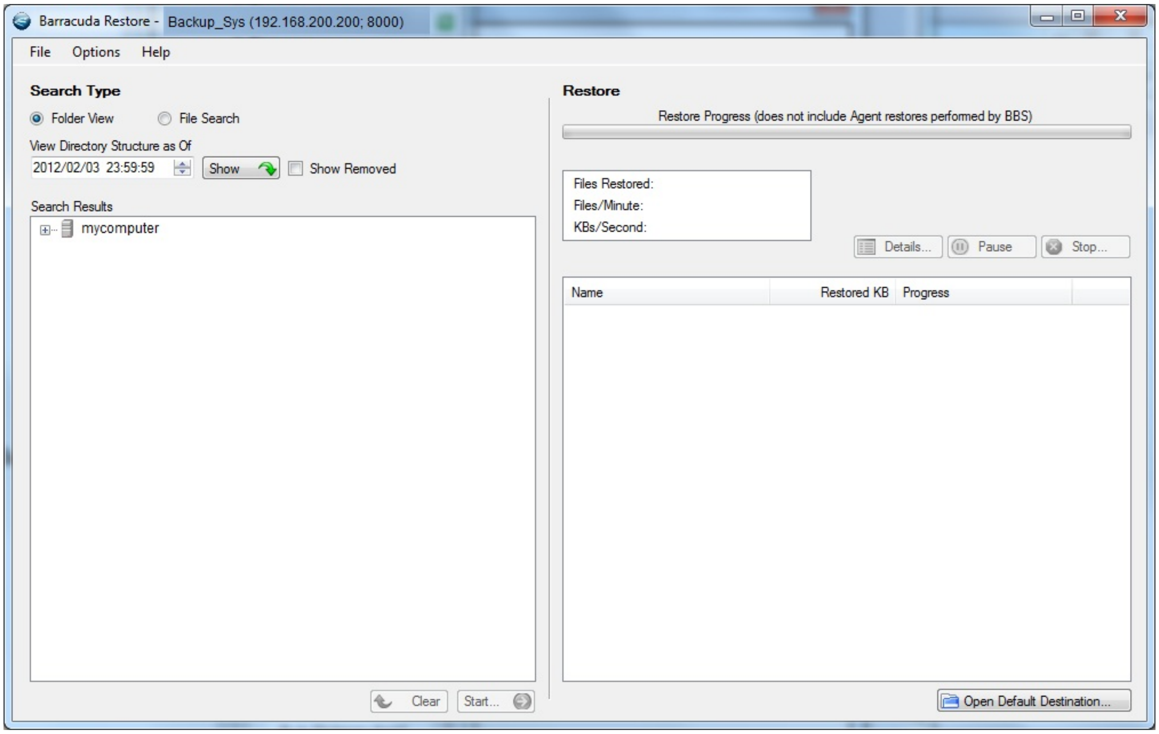
1. In the **User Name** field, enter your Barracuda Backup user name, and enter the associated password in the **Password** field.
2. Select the manner in which to connect:
   - **Connect using Barracuda Cloud**-Connect to your backed up data stored on the Cloud
   - **Connect Directly to a Barracuda Backup Server**-Restore from a local or offsite Barracuda Backup Server; for improved restoration performance, it is recommended that you restore from a local Barracuda Backup Server.
3. Enter the hostname or IP address, and associated port number.
4. If you use a proxy to access the Internet, click **Proxy** to expand the proxy details section; if you are not using a proxy server, skip to **Step 6**.
5. In the Proxy section, select from the following options:
   - **Use Internet Explorer settings** - Select to access the network address of your proxy server using the Explorer Proxy Settings.
   - **Use custom settings**- Select and enter the proxy server hostname or IP address, and associated port number.
6. Verify your settings, and click **Submit**.
7. Barracuda Restore for Windows launches.

Log In

Each time you launch Barracuda Restore for Windows or perform an action that requires authentication, you are required to log into the tool. Once you are logged in, you may be required to log in again if you change your connection location.

> ⓘ Your user name and password should be the same for both the Barracuda Backup Server or Barracuda Cloud Control and the offsite location login; this login is identical to the one you use in the Barracuda web interface.

1. Enter your username and password, and click **Submit**.
2. Once you log into the tool, the associated data sources display:


Barracuda Restore - Backup_Sys (192.168.200.200; 8000)
File
Options
Help
Search Type
Restore
Restore Progress (does not include Agent restores performed by BBS)
Search Results
mycomputer
Files Restored:
Files/Minute:
KBs/Second:
Details...
Pause
Stop...
Name
Restored KB
Progress
Clear
Start...
Open Default Destination...

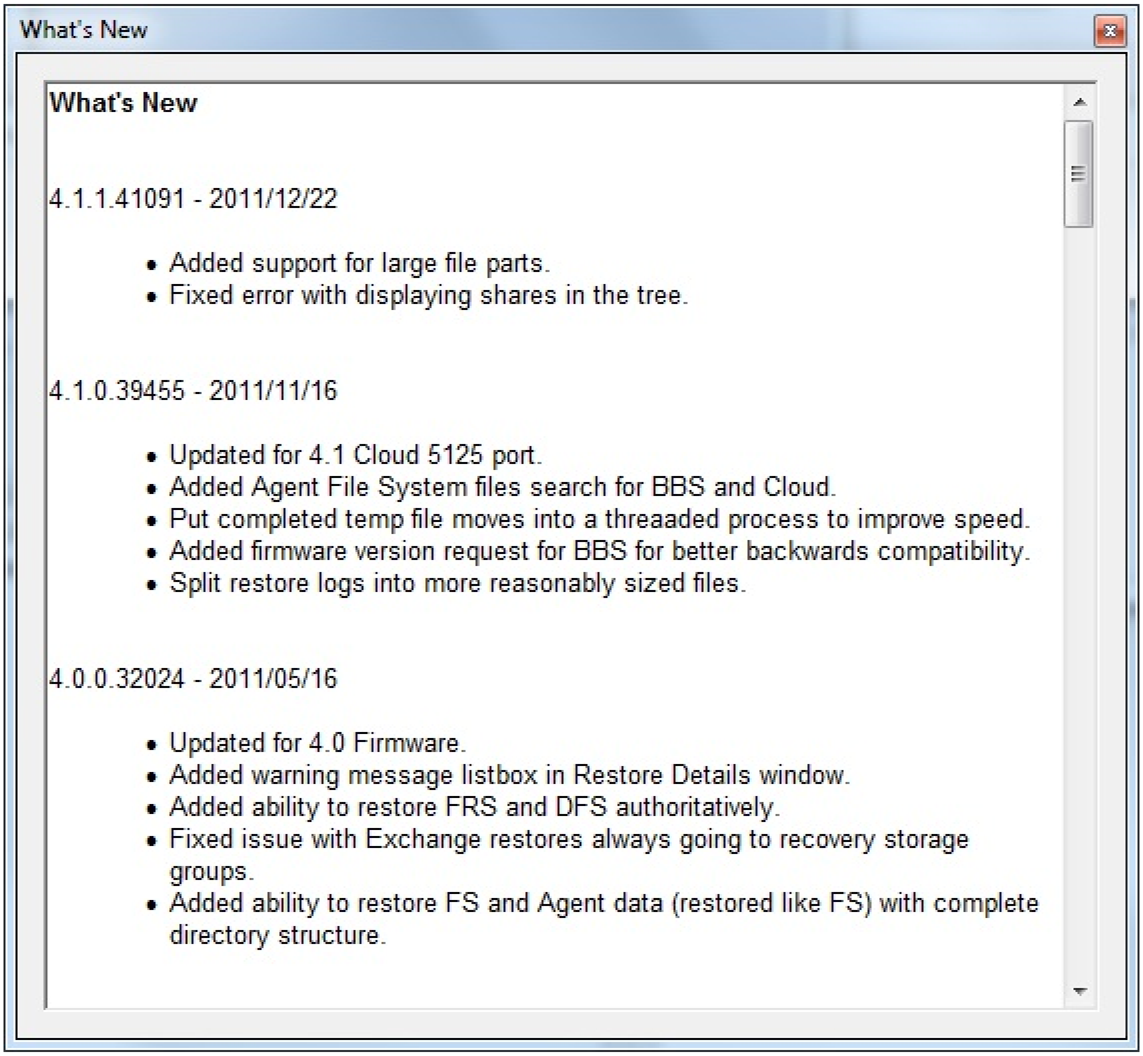
● Folder View ○ File Search

View Directory Structure as Of: 2012/02/03 23:59:59 Show

☐ Show Removed

View New Features List

New features and changes in the application are listed by release in the "What's New" page available from **Help > What's New**:



What's New

4.1.1.41091 - 2011/12/22

- Added support for large file parts.
- Fixed error with displaying shares in the tree.

4.1.0.39455 - 2011/11/16

- Updated for 4.1 Cloud 5125 port.
- Added Agent File System files search for BBS and Cloud.
- Put completed temp file moves into a threaaded process to improve speed.
- Added firmware version request for BBS for better backwards compatibility.
- Split restore logs into more reasonably sized files.

4.0.0.32024 - 2011/05/16

- Updated for 4.0 Firmware.
- Added warning message listbox in Restore Details window.
- Added ability to restore FRS and DFS authoritatively.
- Fixed issue with Exchange restores always going to recovery storage groups.
- Added ability to restore FS and Agent data (restored like FS) with complete directory structure.

Modify Backup Server Location

In general, do *not modify your backup server location unless directed to do so by Barracuda Networks Technical Support*. If directed to do so, you can specify a different source location from which to restore data by going to **Options > Backup Servers**:

- **Cloud** - Click to replace the current hostname/IP address with a cloud connection name and associated port number.
- **Local BBS** - Click to select a Barracuda Backup Server, and automatically connect all of all associated local data sources.
- **Manual** - Click to replace the current hostname/IP address with a different connection name and associated port number; *do not* use this setting unless instructed to do so by Barracuda Networks Technical Support.

How to Customize Barracuda Restore for Windows

This article refers to Barracuda Backup firmware version 4.3 and earlier *only*.

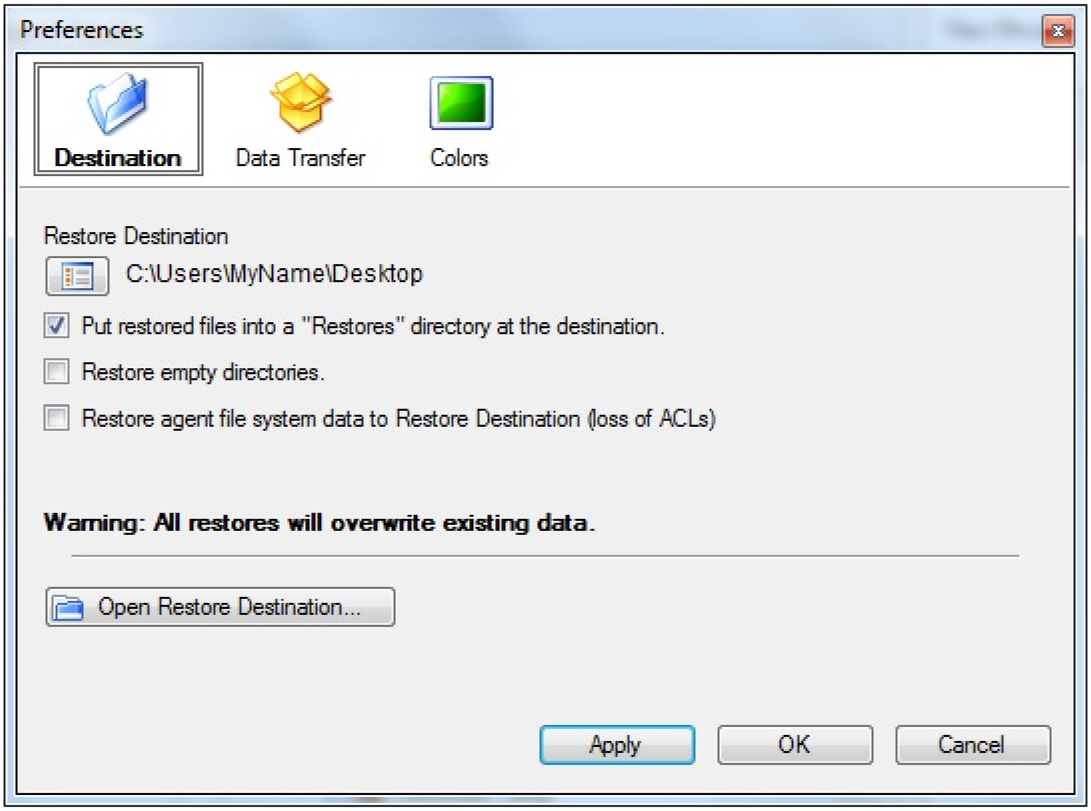
Customize Your View

Use the **Preferences** menu to customize behavior and appearance of **Barracuda Restore Tool for Windows**. From the **Options** menu, click **Preferences**, and select the options you wish to customize. Once you change a setting, click **Apply** to apply your change and continue customizing the **Barracuda Restore Tool for Windows**, or click **OK** to apply your changes and close the dialog box. You can customize the following:

- Destination
- Data Transfer
- Colors

Destination

Use the **Destination** page to specify the default restore destination and to select restore options:



Restore Destination
C:\Users\MyName\Desktop

☑ Put restored files into a "Restores" directory at the destination.

☐ Restore empty directories.

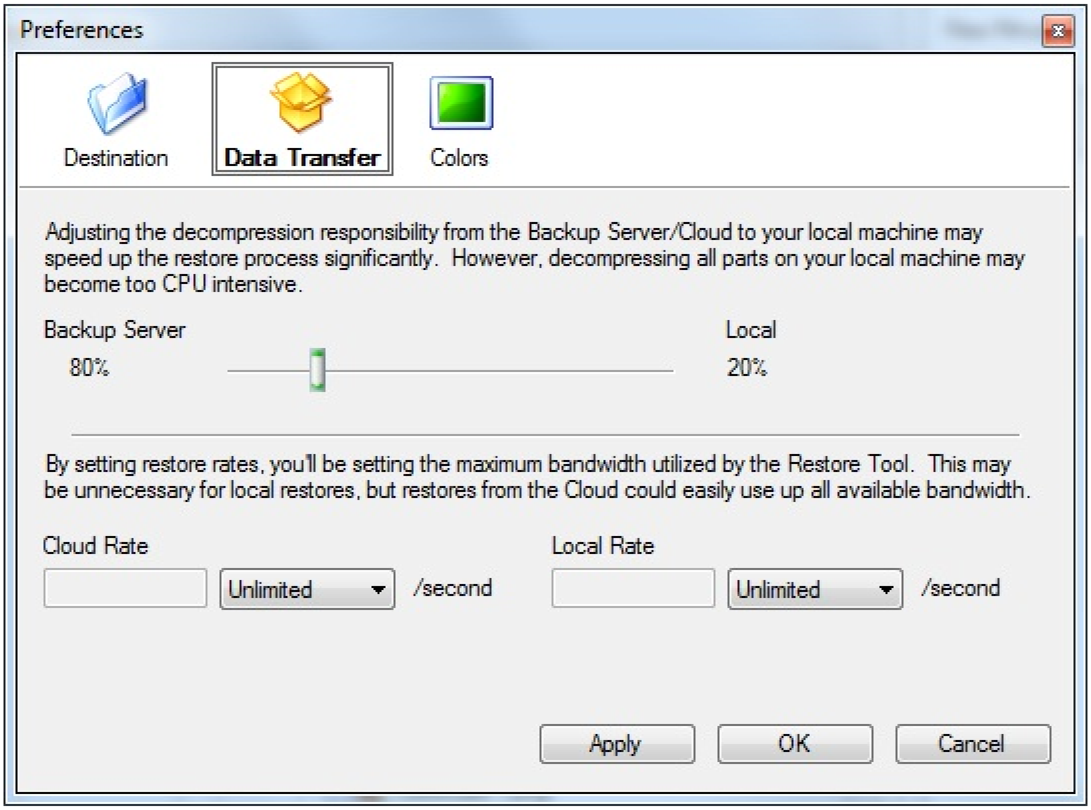
☐ Restore agent file system data to Restore Destination (loss of ACLs)

Warning: All restores will overwrite existing data.

- **Restore Destination** - Click on the **Restore Destination** icon to navigate to and select (or create) the default restore location
- **Put restored files into a "Restores" directory at the destination** (turned on by default) **-** When turned on, restored files are automatically added to a **Restores** folder int he default restore location
- **Restore empty directories** - Turn on to restore empty directories during file restoration
- **Restore agent file system data to Restore Destinations (loss of ACLs)-**Turn on to restore agent directories and files to the default restore location; note that the user permissions on the original folder system are *not* retained
- **Open Restore Destination** - Click to open the default restore folder on your local system

Data Transfer

Use the **Data Transfer** page to balance the workload during a restore between the restoration source location and your local system:



Adjusting the decompression responsibility from the Backup Server/Cloud to your local machine may speed up the restore process significantly. However, decompressing all parts on your local machine may become too CPU intensive.

Backup Server 80%

Local 20%

By setting restore rates, you'll be setting the maximum bandwidth utilized by the Restore Tool. This may be unnecessary for local restores, but restores from the Cloud could easily use up all available bandwidth.

Cloud Rate: Unlimited /second

Local Rate: Unlimited /second

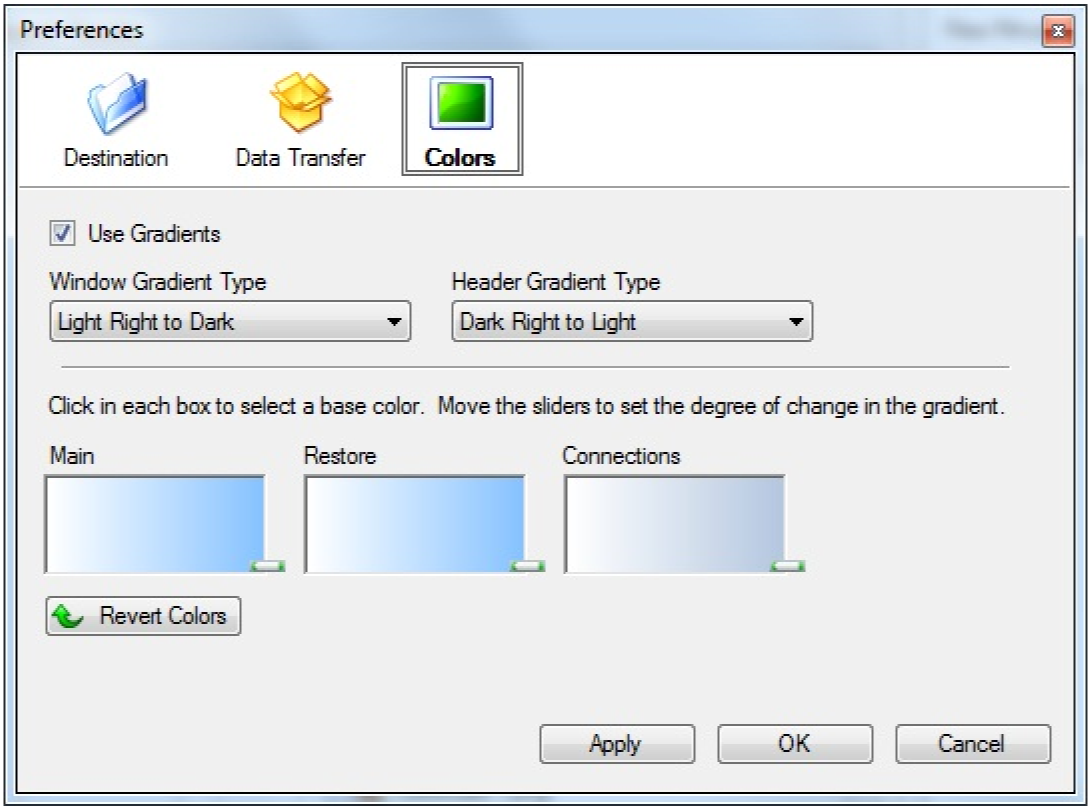
- **Backup Server** - Drag the slide bar to adjust the decompression load between the Barracuda Backup Server/Cloud to your local system

> ⓘ For improved restoration performance, you may wish to adjust the decompression from the Barracuda Backup Server/Cloud to your local system. This allows the parts being restored to come across compressed, and therefore, faster as the source does not have to perform decompression. The local system can then decompress the parts and assemble the files. However, decompressing all parts on your local machine is not recommended as this may become too CPUintensive.

- **Cloud Rate** - Specify the maximum bandwidth restore rate for the source; specify the rate per second as Unlimited, or in Kilobits, Kilobytes, Megabits, or Megabytes
- **Local Rate** - Specify the maximum bandwidth restore rate for the local system; specify the rate per second as Unlimited, or in Kilobits, Kilobytes, Megabits, or Megabytes

Colors

In the **Colors** page you specify whether to use gradient colors to personalize the application in place of the default Windows system colors; by default gradient color is turned off:



☑ Use Gradients

Window Gradient Type: Light Right to Dark

Header Gradient Type: Dark Right to Light

Click in each box to select a base color. Move the sliders to set the degree of change in the gradient.

- **Use Gradients** - Turn on to customize gradient display settings; note that adding gradients to the application settings *does not* affect restoration speed.
- Type display-When **Use Gradients** is turned on, the application detects whether the selected luminosity works best with white or black text, and adjusts the label text color accordingly. If your color selection is "too middle of the road", the application adjusts to the closest acceptable luminosity. Depending on whether you have selected a light or dark color, the gradient fades from your selection to white or black respectively, preventing a gradient that interferes with label text.
- **Revert Colors** - When **Use Gradients** is turned on, you can click in the **Main**, **Restore**, or **Connections** box to select a new base color; to restore the base color to the original value, click **Revert Colors**

> ⓘ If you customize and save your gradients, and then turn off gradients, your settings are not overwritten; however, if you click **Revert Colors** and then click **Apply**, your settings are lost.

How to Run Barracuda Restore for Windows

> This article refers to Barracuda Backup firmware version 4.3 and earlier *only.*

The Barracuda Restore tool is a Windows-based client that allows you to restore data from your local Barracuda Backup Server, a remote Barracuda Backup Server, or from Barracuda Cloud Control. Barracuda Restore for Windows:

- Is recommended if the Internet connection is unavailable and you have to restore data from local Barracuda Backup Server
- Is the only method that can do offline restores
- Does not restore message-level emails
- Can restore data that was backed up by the Barracuda Backup Agent to an alternate location
- Provides option to include or exclude file attributes (metadata) permissions, creation time, etc.

To run Barracuda Restore for Windows:

1. Download and install the Barracuda Restore Tool from the **SUPPORT > Software Downloads** page.
2. Go to **Start > All Programs > Barracuda > Barracuda Restore for Windows**.
3. You can choose to authenticate to a Barracuda Cloud Storage, or to a remote or local Barracuda Backup Server. Your account must have administrator rights to use the Barracuda Restore tool. The username and password are the same as those used to access the Barracuda Backup web interface.
4. Follow the on-screen instructions to select a source for the data to be restored and restore your data. If you restore the data back to the

original location, file attributes are retained. If the data is restored to an alternate location, the file attributes are removed.

How to Restore Data Using Barracuda Restore for Windows

This article refers to Barracuda Backup firmware version 4.3 and earlier *only.*

In this article:

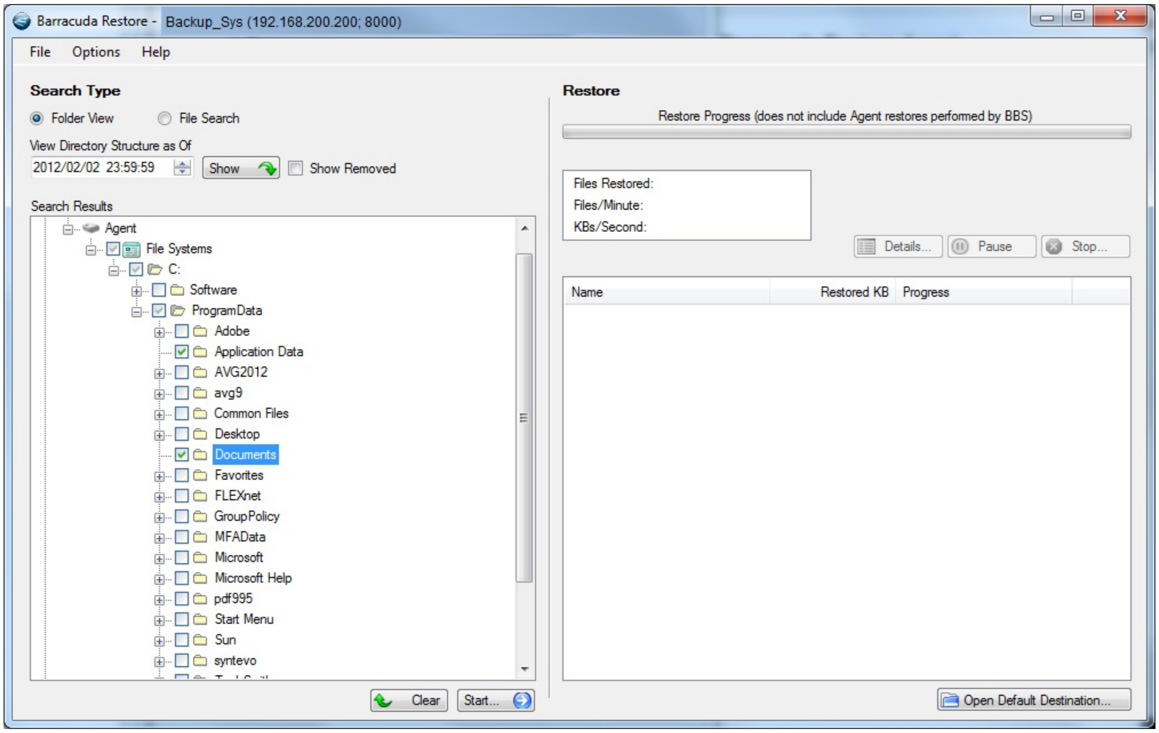
- Select Data for Restoration
- Restore Files
- Restore Logs

Select Data for Restoration

Use Barracuda Restore for Windows to restore data from your local Barracuda Backup Server, a remote Barracuda Backup Server, or from Barracuda Cloud Storage. To restore a directory, or multiple directories or files, from the same date and time, use the **Folder View** option. To search for a specific file or set of files for restoration, use the **File Search** option.

Turn on **File Search** to search for a specific file or set of files you wish to restore:
Display Folders

This view displays the folder tree of your backed up data as it existed at a particular point in time:



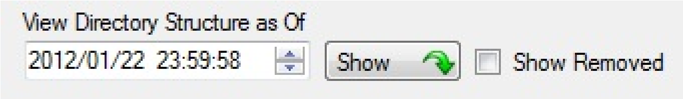
Barracuda Restore - Backup_Sys (192.168.200.200; 8000)
File
Options
Help
Search Type
● Folder View
○ File Search
View Directory Structure as Of
2012/02/02 23:59:59
Show
☐ Show Removed
Search Results
Agent
☑ File Systems
☑ C:
☐ Software
☑ ProgramData
☐ Adobe
☑ Application Data
☐ AVG2012
☐ avg9
☐ Common Files
☐ Desktop
☑ Documents
☐ Favorites
☐ FLEXnet
☐ GroupPolicy
☐ MFAData
☐ Microsoft
☐ Microsoft Help
☐ pdf995
☐ Start Menu
☐ Sun
☐ syntevo
Clear
Start...
Restore
Restore Progress (does not include Agent restores performed by BBS)
Files Restored:
Files/Minute:
KBs/Second:
Details...
Pause
Stop...
Name
Restored KB
Progress
Open Default Destination...

Use the following options in the **Folder View**:

- **Show Removed** - Turn on to select from previously deleted directories and files. When turned on, click **Show** to update the **Search Results** pane with all files, including those that were previously removed, based on the specified date and time range
- **View Directory Structure as Of** - Select the date and time range, and click S**how** to update the Search Results pane based on your selections
- **Clear** - Click to deselect all files and folders in the **Search Results** pane

Select those files and folders you wish to restore; note that when you *turn on* a folder, all files and folders contained within that folder are selected, and when you *turn off* a folder, all files and folders within that folder are deselected. To clear all currently selected files and folders, click **Clear**.
Revision Date

To view file revisions by date and time, select the date and time range in the **View Directory Structure as Of** filed, and click **Show** to update the **Search Results** pane:


View Directory Structure as Of
2012/01/22 23:59:58

☐ Show Removed

File Restore

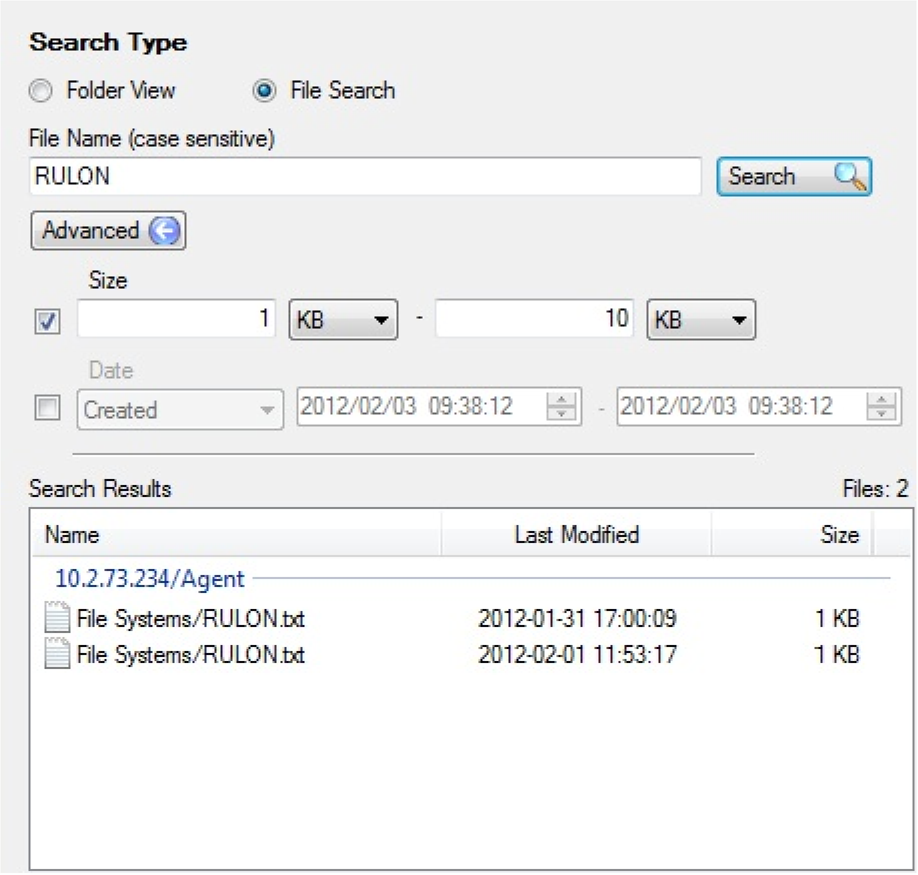
You can restore a single file from the **Folder View**.

1. Navigate to the file(s) you wish to view.
2. To view revisions on a single file by date including file size, navigate to and doubleclick the desired file name to open the **Revisions** window.
3. In the **Revisions** window, select the desired revision, and click **Restore** to restore the selected file.

Note: When restoring multiple versions of a file, the entire directory structure is maintained, allowing multiple versions of the same file without overwriting each revision as long as data is not restored to its original location via the agent.

File Search

Turn on **File Search** to search for a specific file or set of files you wish to restore:


Search Type
○ Folder View ● File Search
File Name (case sensitive): RULON

Size
☑ 1 KB - 10 KB
Date
☐ Created 2012/02/03 09:38:12 - 2012/02/03 09:38:12

Search Results — Files: 2

Name	Last Modified	Size
10.2.73.234/Agent		
File Systems/RULON.txt	2012-01-31 17:00:09	1 KB
File Systems/RULON.txt	2012-02-01 11:53:17	1 KB

Note that search criteria is *case sensitive.*

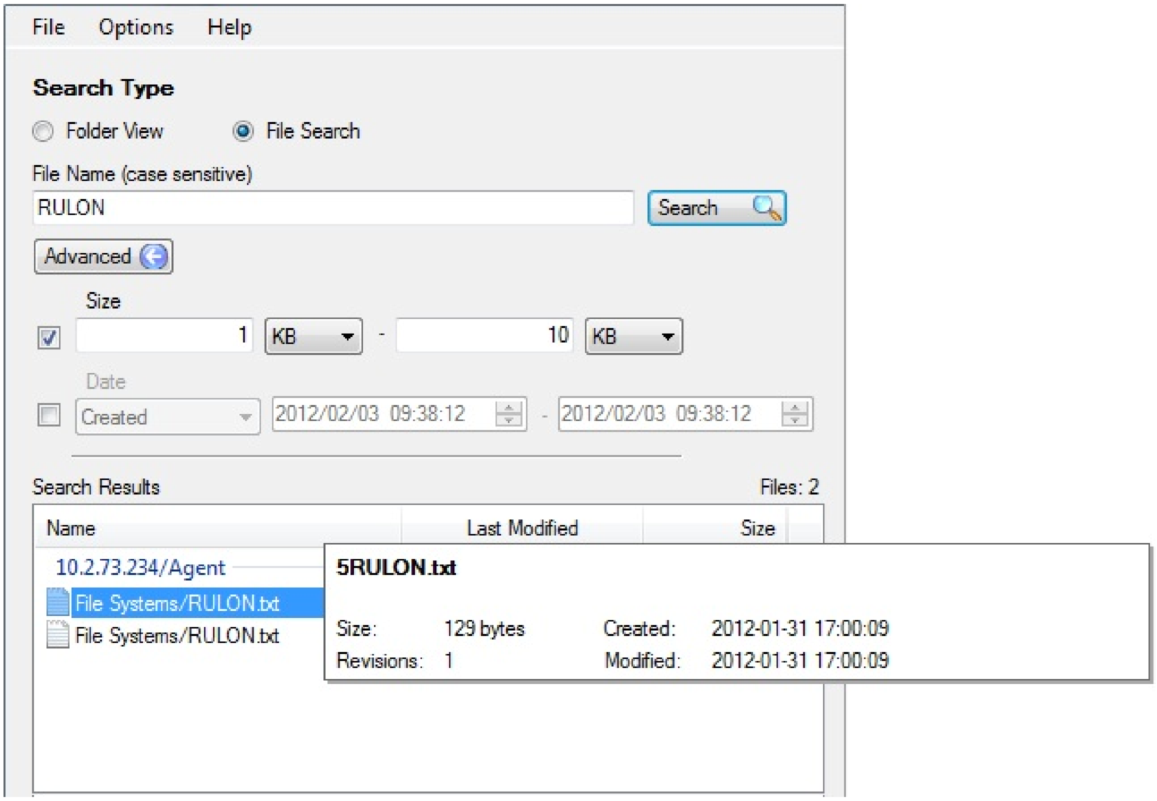
To search for a backed up file you wish to restore, select from the following options:

- Basic Search - Enter all or a portion of the **File Name**, and click **Search**
- Advanced Search - Enter all or a portion of the **File Name**, click **Advanced**, and then turn on the desired options before you click **Search**:
    - **Size** - Turn on to specify the file size range in **Bytes**, **KB**, **MB**, or **GB**
    - **Created, Last Modified,** or **Removed** - Select the date range type, and then adjust the date range to match the selected criteria

Once the search is complete, a maximum of 500 records return; to limit the number of files returned, click **Advanced** and refine the size and/or date range, and then run the file search once again.

In the **Search Result** pane, you can view more information about a file:

- Click once on a file to view file size, number of revisions, and creation/modification date:



Search Type

○ Folder View ● File Search

File Name (case sensitive): RULON

Size ☑ 1 KB - 10 KB

Date ☐ Created 2012/02/03 09:38:12 - 2012/02/03 09:38:12

Search Results Files: 2

Name	Last Modified	Size
10.2.73.234/Agent		
File Systems/RULON.txt		
File Systems/RULON.txt		

5RULON.txt

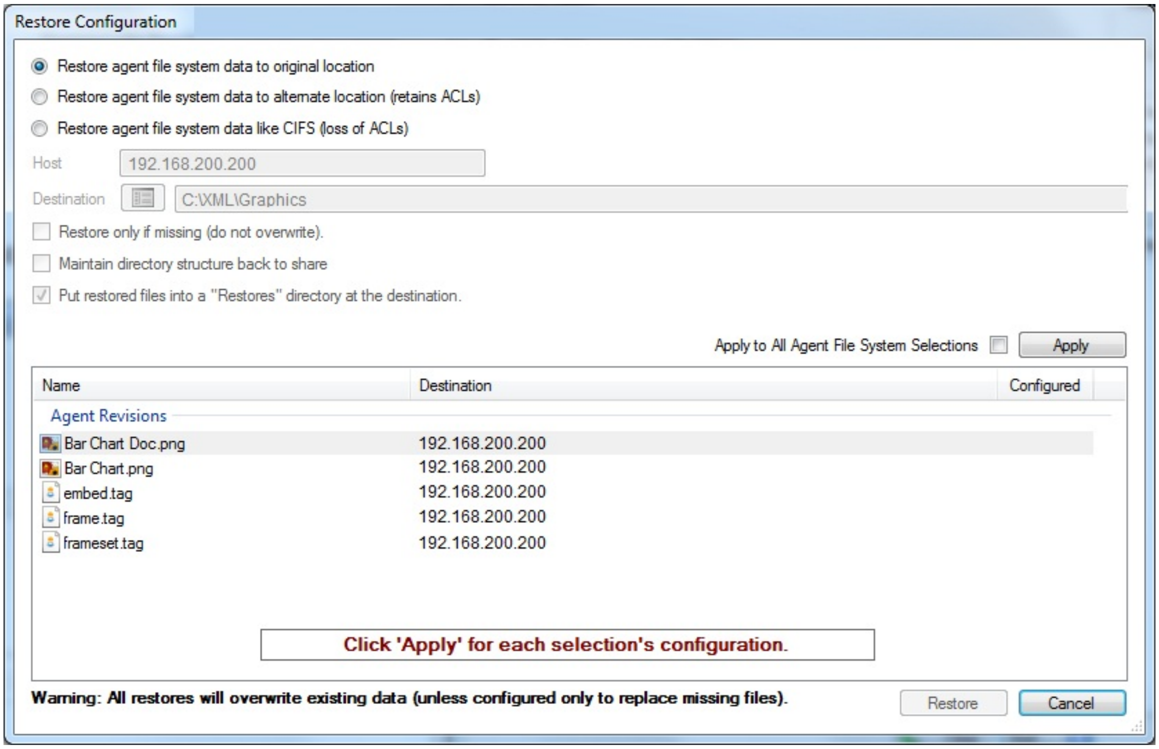
Size:	129 bytes	Created:	2012-01-31 17:00:09
Revisions:	1	Modified:	2012-01-31 17:00:09

- Double-click on a file to view all revisions by date, and optionally select to restore a revision directly from the window.

Restore Files

Once you select the desired files for restoration,

1. Click **Start** to bring up the **Restore Configuration** dialog box where you specify Agent Directory and Agent Revision restore locations:



● Restore agent file system data to original location

○ Restore agent file system data to alternate location (retains ACLs)

○ Restore agent file system data like CIFS (loss of ACLs)

Host: 192.168.200.200

Destination: C:\XML\Graphics

☐ Restore only if missing (do not overwrite).

☐ Maintain directory structure back to share

☑ Put restored files into a "Restores" directory at the destination.

Apply to All Agent File System Selections ☐

Name	Destination	Configured
Agent Revisions		
Bar Chart Doc.png	192.168.200.200	
Bar Chart.png	192.168.200.200	
embed.tag	192.168.200.200	
frame.tag	192.168.200.200	
frameset.tag	192.168.200.200	

Click 'Apply' for each selection's configuration.

Warning: All restores will overwrite existing data (unless configured only to replace missing files).

2. Click on a file name, and select from the available configuration options:
   - **Restore agent file system data to original location -** Select to restore the data to the original file system location. By default, files are restored to the **Restores** folder, for example, **User Name > My Documents > Restores**; to open the default restore

folder, in the main **Barracuda Restore** window, click **Open Default Destination**.

- **Restore agent file system data to alternate location (retain ACLs)** - Select to specify an alternate location to which to restore the data; note that the user permissions on files and folders are retained.
- **Restore agent file system data like CIFS (loss of ACLs)** - Select to restore the agent file system data, including windows file sharing-related data. You can identify an alternate location to which to restore the data, and then specify:
  - **Restore only if missing (do not overwrite)**
  - **Maintain directory structure back to share**
  - **Pub restored files into a "Restores" directory at the destination**
- **Apply to All Agent File System Selections** - Turn on if the selected configuration options apply to all files

To specify the restore location,

1. Select from the available restore locations and configuration options.
2. In the list of items for restoration, select the item on which to set the configuration options, and click **Apply**.
3. Once you apply the restore location to an item, verify a check mark displays to the right of the item.
4. If the configuration options apply to all files, click **Apply to All Agent File System Selections**, and click **Apply**.
5. Click **Restore**. The window closes and the restoration begins.

Note: You must specify the restore location for all items before you can complete the restore process.

Once the restoration begins, **Restore Progress** displays in the tool window. As the restore progresses, the overall restoration progress and individual file restoration progress displays as progress bars including an in-progress counter of total files restored, files per minute, and kilobytes per second. If errors are encountered during the restore process, click **Restore Logs** and open the latest restore log for more information.

View, Pause, or Stop Restoration

While the restoration is in progress, click the **Details** icon to view realtime important restoration details about restoration progress such as path issues and restore failures. This allows you to determine if a restore needs to be canceled and redefined. Additionally, you can turn on the following options in the **Details** window:

- **Rate Limit** - Click to specify the restoration rate limit per second; specify as unlimited, or in kilobits, kilobytes, megabits, or megabytes
- **Open this window at the start of each restore** - Turn on to automatically launch the **Details** window each time you start a restore

While the restoration is in progress, you can also select:

- **Pause/Play** - Click to suspend/resume restoration
- **Stop** - Click to end the restoration process and remove partially restored files

Restore Logs

Once a restore is complete, paused, or stopped, the **Restore Completed** dialog box displays the restore statistics. From this view you can click **Restore Logs** to view restore details. A restore log is generated each time you perform a restore, and is named based on the restoration date and time. The log file is stored in a sub-folder of the **Barracuda Restore for Windows** folder. For example,
`C://Program Data/Barracuda/Barracuda Restore for Windows/Restore Logs`

ⓘ Log files are always stored in this location regardless of the specified restore location.

You can also access the **Restore Logs** folder from the **Help > Restore Logs** folder.

View Error Logs

Error logs are generated *only* if an error is encountered during a file or folder search, or during restoration. File naming is based on the date and time of the error, and the error log file is stored in a sub-folder of the **Barracuda Restore for Windows** folder. For example,
`C://Program Data/Barracuda/Barracuda Restore for Windows/Error Logs`

REPORTS Page

This article refers to Barracuda Backup firmware release 5.0 and higher, except where noted.

In this article:

- Backup Reports
- Restore Report
- Large Items Report
- Audit Log Report

- User Activity Reports

Backup Reports

Barracuda Backup provides a detailed report for each backup that is run. Backup reports can be accessed from the **REPORTS > Backup** page of the Barracuda Backup web interface. In addition, any back up process that is currently running is also displayed from this page. Backup reports include details about the backup such as when the backup started, duration, size, if there were any errors or warnings, and any new, changed, or removed items. Reports also include links to each backed up file to view or download the item from the report.

Click **Details** to view recent activity in chart form. You can also view a list of backed up files including the number of new, changed, and removed files, as well as a list of any errors encountered during backup.

If a backup is currently in progress, the **REPORTS > Backup** page displays this information and allows you to cancel the backup.

Click **View Past Reports** to access archived backup reports in the **Backup (Archived)** page. You can specify the number of reports you wish to display on the page, or enter a date range and click **Update** to display the archived reports.

Click on the report to view report details, and specify whether to show new, changed, or removed files. Additionally, you can click on a file name to restore the file through the **RESTORE > Restore Browser** page.

Restore Report

You can view restoration details in the **REPORTS > Restore** page. To specify how you wish to sort the table, click on a heading, and then click on the up/down arrows to the right of each heading to specify either an ascending or descending sort.

Click **Details** to view all details for the selected restoration including any encountered errors. Expand the detail tabs to view specific file errors and a list of restored content.

Large Items Report

Firmware version 5.1 and higher only

The **Large Item** Report is available only in Barracuda Backup firmware version 5.1 and higher.

The **REPORTS > Large Items** page displays a detailed list of large items including the data source and path, original file size, and deduplicated backup size. From the **Sources** drop-down menu, you can select to view large items by individual source, by Agent, or for all sources. To further refine the report, enter a string in the **Filename contains** field, and click **Filter**. The report displays only those items matching the **Filename contains** value for the selected source.

Audit Log Report

The **REPORTS > Audit Log** page displays a report of all activities on the Barracuda Backup web interface by time and date, by user, and by action. Logged activity includes log on authentication, firmware update, changes to settings, changes to account information, and more. Click the **Details** icon for additional information for a specific activity.

In the top pane, you can specify the following:

- Select a specific user or display logs for all users
- Specify whether to include log on authentication activities
- Date range of logs to display

User Activity Reports

Firmware version 5.0 and earlier only

The **User Activity** Report is available only with Barracuda Backup firmware version 5.0 and earlier.

The **REPORTS > User Activity** page displays activity logs of users accessing the Barracuda Backup web interface. Logged activity includes log on authentication, firmware update, changes to settings, changes to account information, and more. Mouse-over an entry for additional information.

In the top pane, you can specify the following:

- Number of logs to display

- Date range of logs to display
- Select a specific user or display logs for all users
- Specify whether to include log on authentication in the logs

Once you make changes, click **Update** to display user activity based on your new settings.

SYSTEM Page

This article refers to firmware version 5.0 and higher, except where noted.

Use the **SYSTEM** page to manage the Barracuda Backup firmware version and settings, and access software downloads.

Location	**Description**	**Related Articles**

SYSTEM > Firmware	• Displays the current version of the installed firmware
	• Allows you to set your **Firmware Upgrade Policy** and install a new firmware release based on the selected policy:
	  ◦ **Legacy Release** - Access a previously installed version of the firmware; *do not select this option unless directed to do so by* Barracuda Networks Technical Support.
	  ◦ **General Release** - The latest generally available version of the firmware available for use on Barracuda Backup.
	  ◦ **Early Release** - The newest firmware versions available for early access to Barracuda Backup.
	• To update the firmware, click **Firmware Available**; if a newer version is available, you are prompted to download and apply the new firmware.
	• View Barracuda Backup release notes including new features and resolved issues.	

SYSTEM > Barracuda Backup Server Settings	Specify the Barracuda Backup Settings including: - **Backup Server Name** - Enter a name to identify the Barracuda Backup Server in the web interface. - **Backup Server Time Zone** - From the drop-down menu, select the time zone where the Barracuda Backup Server is located. - **Barracuda Backup Server Location** - Enter the Barracuda Backup Server physical location details - **Backup Server Display Group** - If you have created display groups, from the drop-down menu, select the group in which to display the Barracuda Backup Server. Click **Manage your display groups** to go to the **ADMIN > Display Groups** page where you can create and manage display groups.	- How to Configure Barracuda Backup - Display Groups page
SYSTEM > Software Downloads	Download tools for use with Barracuda Backup including the Barracuda Backup Agent.	- Barracuda Backup Agent - Barracuda Linux Backup Agent - Bare Metal Restore - How to Configure Backups
SYSTEM > Advanced Graphs	In firmware version 5.3.00 and higher, in addition to the graphs provided on the **STATUS** page, you can access detailed system performance information on the **Advanced Graphs** page.	

Firmware Page

This article refers to Barracuda Backup version 4.2 or higher.

In this article:

- Firmware Update
- Firmware Notification

Related Articles

- System Management

Firmware Update

Use the **SYSTEM > Firmware** page to select the firmware upgrade policy:

- **Current Installed Version** - Displays the currently installed firmware version
- **Firmware Upgrade Policy** - Select the release stage you want to update to the latest firmware:
  - **Legacy Release** - Access a previously installed version of the firmware; *do not select this option unless directed to do so by Barracuda Networks Technical Support.*
  - **General Release** - The latest generally available version of the firmware available for use on Barracuda Backup.
  - **Early Release** - The newest firmware versions available for early access to Barracuda Backup.
- **Firmware Available** - Specifies the latest firmware version available based on the selected **Upgrade Policy**
- **Upgrade Now** - If a newer version of firmware is available, click **Upgrade Now** to upgrade the firmware
- **View release notes** - Click to view the Barracuda Backup release notes

Firmware Notification

If a newer version of firmware is available, once you log in to Barracuda Backup, the **Status** page displays a notification banner across the top of the page. Click **Upgrade Now** to immediately begin the firmware upgrade, or click **Dismiss** to hide the banner until the next time you log in to the web interface.

ⓘ If a backup job is running and you select to upgrade the firmware, the firmware upgrade is queued until the existing job is completed.

BBS Settings Page

This article refers to Barracuda Backup version 4.2 or higher.

Use the **SYSTEM > BBS Settings** page to view or modify the Barracuda Backup Server details including server name, time zone, physical location, and display group:

- **Backup Server Name** - Name used to identify the currently selected Barracuda Backup Server in the web interface
- **Backup Server Time Zone** - The time zone where the currently selected Barracuda Backup Server is located
- **Backup Server Location** - The physical location of the Barracuda Backup Server including city, state, and country
- **Backup Server Display Group** - The display group in which the Barracuda Backup Server resides
- **Manage your display groups** - Click to add or remove a display group in the **ADMIN > Display Groups** page

Software Downloads Page

This article refers to Barracuda Backup version 4.2 or higher.

Go to the **SYSTEM > Software Downloads** page to download tools for use with Barracuda Backup including:

- Barracuda Bare Metal Live CD
- Barracuda Backup Agent (Windows)
- Barracuda Backup Agent (Linux)
- Barracuda GroupWise Trusted Application Key Generator

Advanced Graphs Page

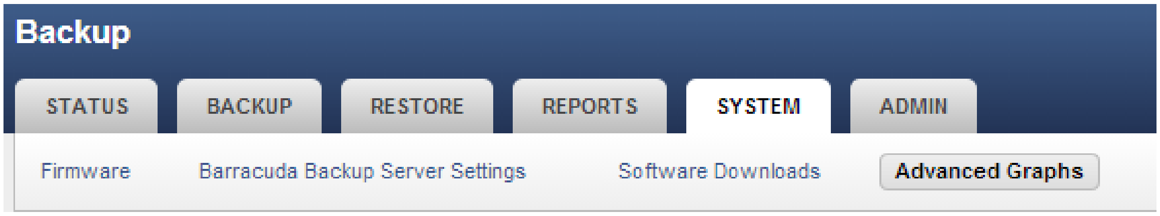
This article applies to Barracuda Backup version 5.3.00 or higher.

In this article:

- View Advanced Graphs
- Local Ethernet Traffic
- Barracuda Central Bandwidth
- Transfer Efficiency
- Node Latency
- Disk Space
- Queue Size
- Queue Count
- Processor Utilization
- Metadata Queue Length

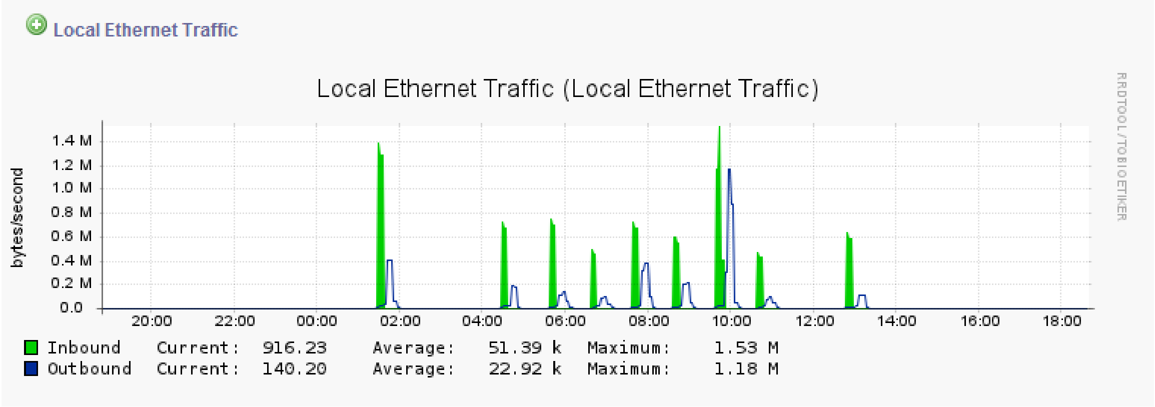
View Advanced Graphs

To view Advanced Graphs, log in to the web interface, select the Barracuda Backup Server in the left pane, and go to the **SYSTEM > Advanced Graphs** tab:


Backup
STATUS
BACKUP
RESTORE
REPORTS
SYSTEM
ADMIN
Firmware
Barracuda Backup Server Settings
Software Downloads
Advanced Graphs

Local Ethernet Traffic

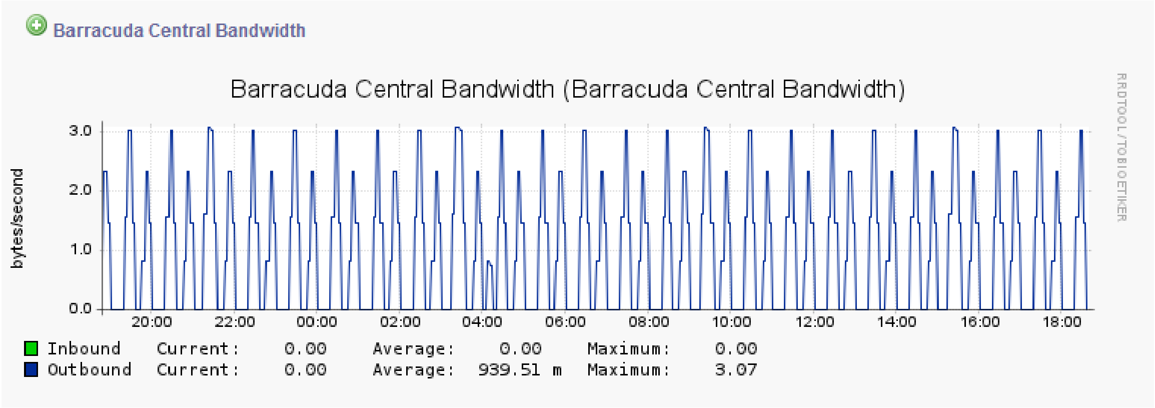
The Local Ethernet Traffic graph presents inbound and outbound network traffic for the selected Barracuda Backup Server:



```
🟩 Inbound   Current:  916.23    Average:  51.39 k   Maximum:    1.53 M
🟦 Outbound  Current:  140.20    Average:  22.92 k   Maximum:    1.18 M
```

Barracuda Central Bandwidth

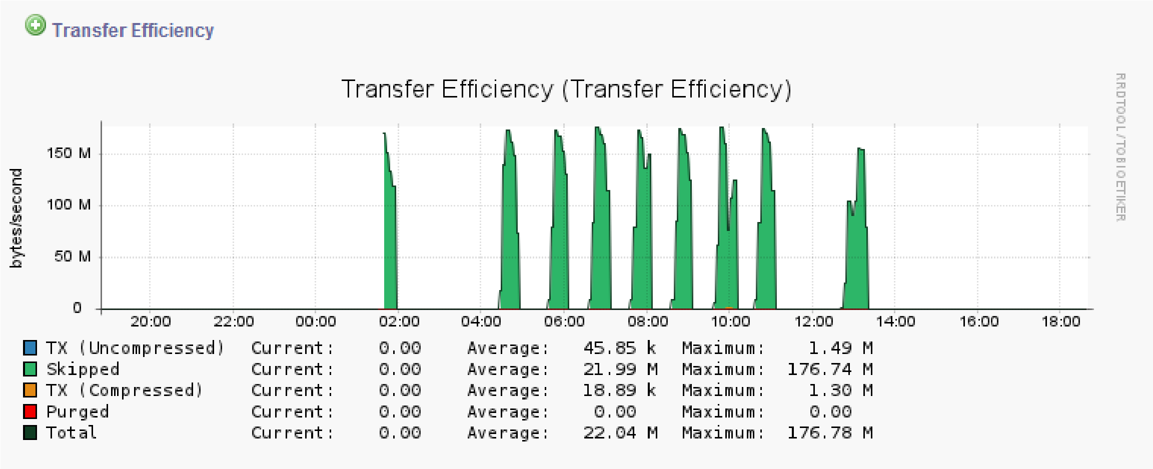
The Barracuda Central Bandwidth graph represents the bandwidth utilization from the Barracuda Backup Server to the Barracuda Networks Cloud Servers:



```
🟩 Inbound   Current:    0.00    Average:    0.00     Maximum:    0.00
🟦 Outbound  Current:    0.00    Average:  939.51 m   Maximum:    3.07
```

Transfer Efficiency

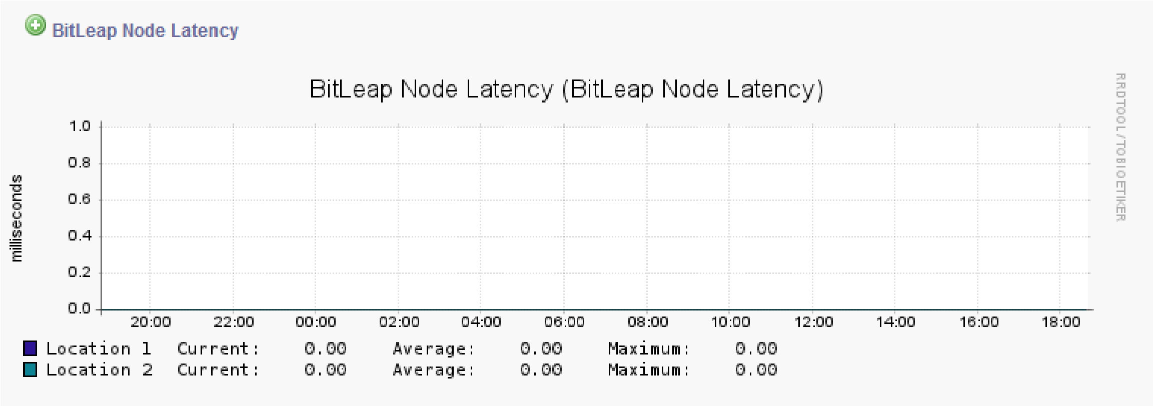
The Transfer Efficiency graph provides a detailed look at data replication from the Barracuda Backup Server to the replication target (Barracuda Cloud or another Barracuda Backup Server). In the graph below, the green shaded area represents the **Skipped** or deduplicated data. The blue, **TX (Uncompressed)**, represents the actual data being transferred and the amount of bandwidth that would be used if compression was not utilized. The orange, **TX (Compressed)**, represents the actual bandwidth utilized, after compression, to send data offsite. The red **Purged** amount refers to data removed from the offsite transfer queue that has already been purged locally:



```
🟦 TX (Uncompressed)  Current:   0.00    Average:   45.85 k  Maximum:    1.49 M
🟩 Skipped            Current:   0.00    Average:   21.99 M  Maximum:  176.74 M
🟧 TX (Compressed)    Current:   0.00    Average:   18.89 k  Maximum:    1.30 M
🟥 Purged             Current:   0.00    Average:    0.00    Maximum:    0.00
⬛ Total              Current:   0.00    Average:   22.04 M  Maximum:  176.78 M
```

Node Latency

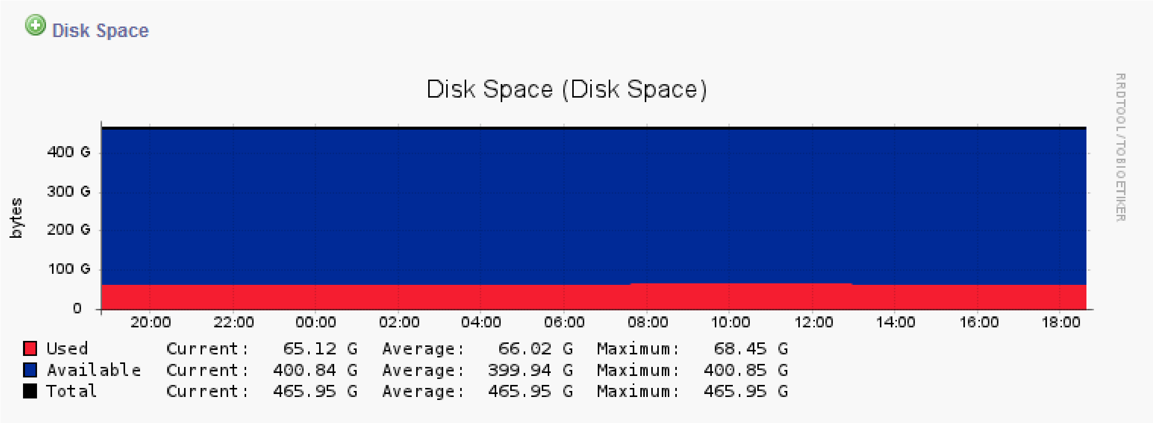
The Node Latency graph represents the latency between the Barracuda Backup Server and the cloud node:



```
🟪 Location 1  Current:   0.00    Average:   0.00    Maximum:   0.00
🟦 Location 2  Current:   0.00    Average:   0.00    Maximum:   0.00
```

Disk Space

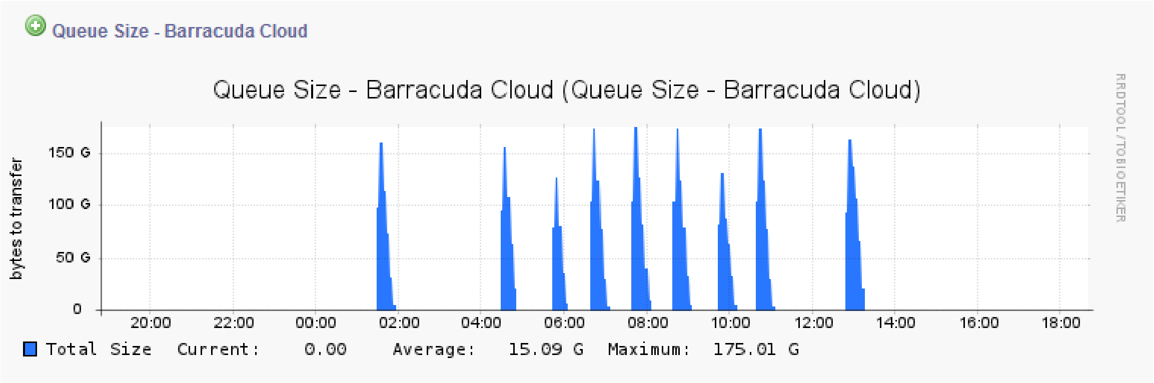
The Disk Space graph provides a detailed account of the amount of disk space that has been used on the Barracuda Backup Server, as well as the remaining available disk space:



```
🟥 Used       Current:   65.12 G  Average:   66.02 G  Maximum:   68.45 G
🟦 Available  Current:  400.84 G  Average:  399.94 G  Maximum:  400.85 G
⬛ Total      Current:  465.95 G  Average:  465.95 G  Maximum:  465.95 G
```

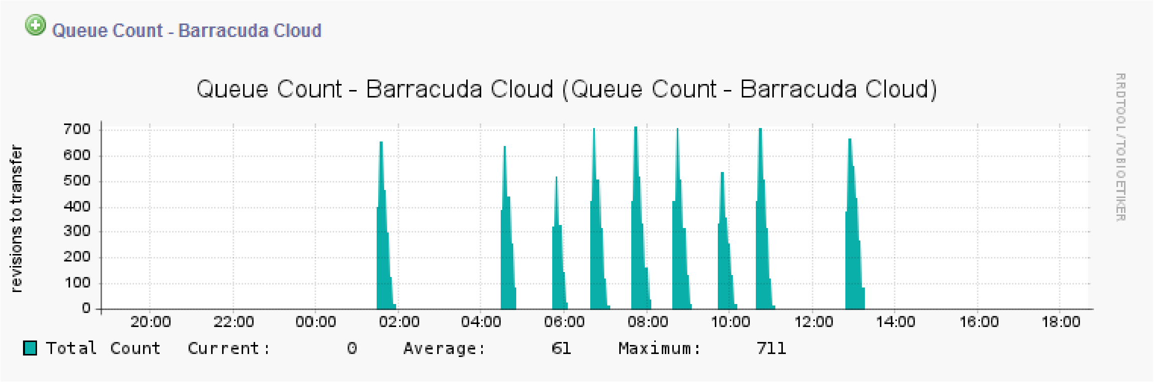
Queue Size

The Queue Size - Barracuda Cloud graph presents a graphical history of the amount of data replicated over time from the Barracuda Backup Server to the Barracuda Cloud:



Queue Count

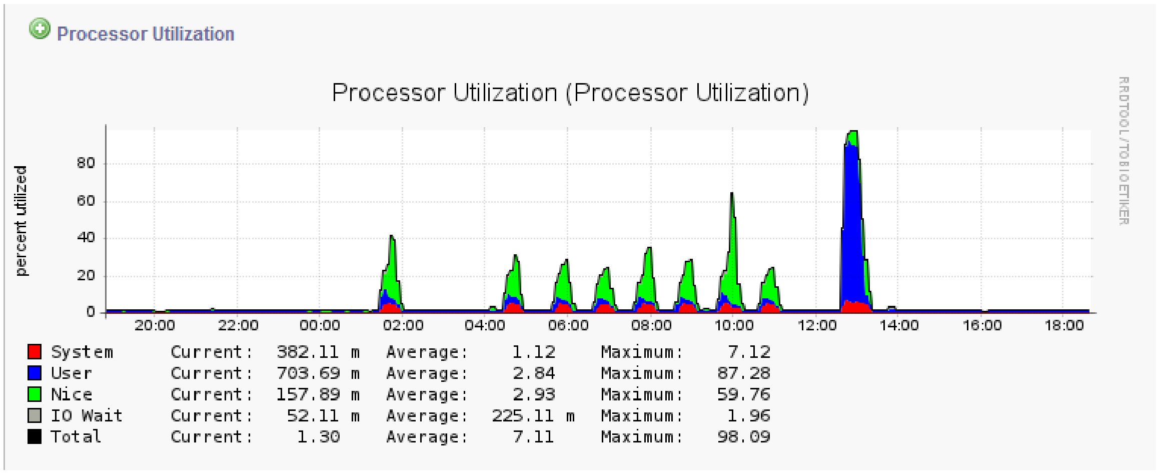
The Queue Count - Barracuda Cloud graph represents the number of parts replicated over time:



Processor Utilization

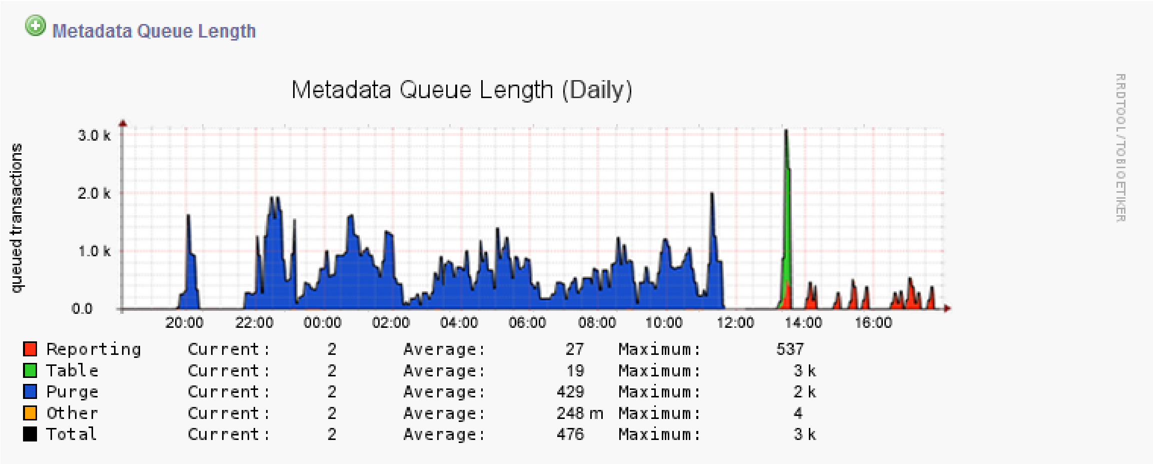
The processor utilization graph represents the following:

- **System** - Percentage of CPU utilization that occurred while executing at the system level (kernel).
- **User -** Percentage of CPU utilization that occurred while executing at the user level (application).
- **Nice** - Percentage of CPU utilization that occurred while executing at the user level with nice priority.
- **IO Wait** - Percentage of time that the CPU or CPUs were idle during which the system had an outstanding disk I/O request.
- **Idle** - Percentage of time that the CPU or CPUs were idle and the system did not have an outstanding disk I/O request.



Metadata Queue Length

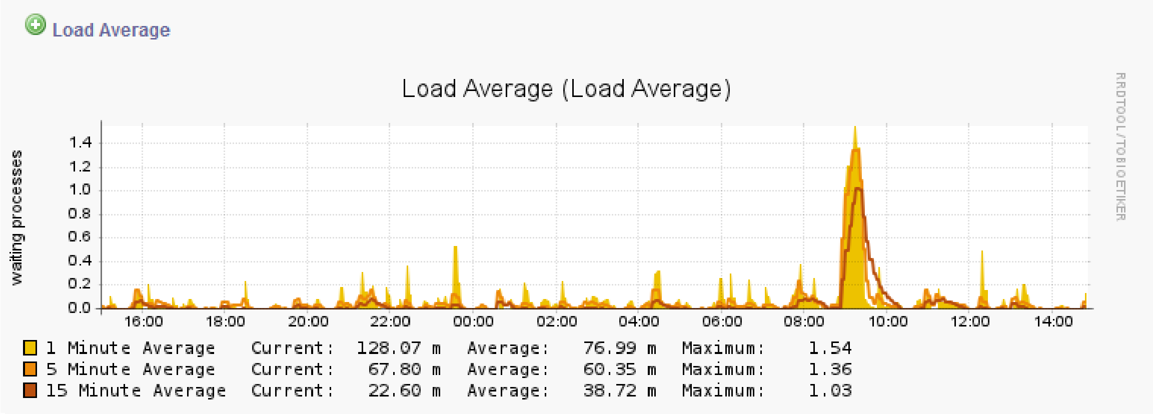
The Metadata Queue Length graph provides a graphical representation of the reporting and statistics data transfer over time:



```
Reporting    Current:   2     Average:    27     Maximum:    537
Table        Current:   2     Average:    19     Maximum:    3 k
Purge        Current:   2     Average:   429     Maximum:    2 k
Other        Current:   2     Average:   248 m   Maximum:    4
Total        Current:   2     Average:   476     Maximum:    3 k
```

Load Average

The Load Average graph details the history of running processes over time:



```
1 Minute Average   Current:  128.07 m  Average:   76.99 m  Maximum:   1.54
5 Minute Average   Current:   67.80 m  Average:   60.35 m  Maximum:   1.36
15 Minute Average  Current:   22.60 m  Average:   38.72 m  Maximum:   1.03
```

ADMIN Page

This article refers to firmware version 5.0 and higher.

Use the **ADMIN** page to configure users, set up email notifications, manage display groups, access documentation, and link a Barracuda Backup Server.

Location	Description	Related Articles

ADMIN > Users	Use this page to administer users that have access to the Barracuda Backup Service web interface. Click the **Edit** icon to modify email notifications, authentication, and permissions for the selected user, or click **Add & Remove Users** to add a new user, edit details for an existing user, or delete a user. If you are an administrator, you can modify your profile in the following manner: 1. Go to **ADMIN > Users**, and click **Add & Remove Users**. 2. Click the **MY PROFILE** tab to change your password, change product notifications, and set the time zone for your user account. 3. Click **Save** to apply your settings.	• Managing Users • Managing Your Account
ADMIN > Email Notifications	Specify the type of email notification for each user: • **Reports** - When selected, an email notification is sent for each backup job. • **Alerts** - When selected, an email notification is sent if a backup job has errors or if your Barracuda Backup Server is offline. • **Notices** - When selected, an email notification is sent when your Barracuda Backup Server software is updated.	• Managing Email Notifications
ADMIN > Display Groups	Add and remove display groups to manage multiple Barracuda Backup Servers.	• Display Groups
ADMIN > Documentation	Access Barracuda Knowledgebase and Barracuda TechLibrary articles.	
ADMIN > Link a Barracuda Backup Server	Link your Barracuda Backup Server to your Barracuda Cloud Control Account.	• Link a Barracuda Backup Server to an Account • Unlink a Barracuda Backup Server

Users Page

Use this page to administer users that have access to the Barracuda Backup Service web interface. Click the **Edit** icon to modify email notifications, authentication, and permissions for the selected user, or click **Add & Remove Users** to add a new user, edit details for an existing user, or delete a user.

If you are an administrator, you can modify your profile in the following manner:

1. Go to **ADMIN > Users**, and click **Add & Remove Users**. From this page you can complete the following actions:
    - Click **Add User** in the **ADMIN** tab to create a new user
    - Click on an existing user name to edit or remove the selected user
2. Click the **MY PROFILE** tab to change your password, change product notifications, and set the time zone for your user account.
3. Click **Save** to apply your settings.

From the Users page, you can:

- Manage Your Account
- Manage User Access
- Manage Product Entitlements

Managing Your Account

Your account with Barracuda Networks gives you access to Barracuda Backup, Barracuda Networks services to which you have a subscription, and any devices added through Barracuda Appliance Control. As long as you are logged in as an administrator, you can add users that can perform administrative tasks. Each user uses their own user name to log in.

In this article:

- Select Account Options
- Community
- Account
- Support
- Verify Service Plan Size

Related Articles
• Create a Barracuda Cloud Control Account • Product Entitlements

Select Account Options

Go to **ADMIN > Users** to perform these account-related tasks:

- Add, edit and remove users, including setting their privileges and start page. When you add a user you can select the services that the user is able to access.
- Update contact and billing information for your Barracuda Cloud Control account.
- View invoices.
- Manage services associated with your account.

Click on the **Backup Service** link on the top left hand side to go to the Barracuda Backup web interface.

Community

Click on **Community** at the top left hand side of the Barracuda Backup web interface to access product forums and add your own feedback. Use forums to discuss and view feature requests. For additional information, refer to Barracuda User Community.

Account

Click on **Account** on the top left hand side of the Barracuda Backup web interface to perform the following tasks:

- Update contact and billing information for your Barracuda Cloud Control account
- Manage user information and specify device access
- View user event log files
- Change your password
- View status of your Barracuda Cloud Control Services
- View invoices
- Specify forum and product notification settings

Support

Click on **Support** on the top left hand side of the Barracuda Backup web interface to perform the following tasks:

- Search Barracuda Networks Knowledgebase solutions
- Access the Barracuda Networks TechLibrary
- Contact Barracuda Networks Technical Support
- Access existing support cases, or open a new case
- Manage your Barracuda Backup Server serial numbers

Verify Service Plan Size

After you have successfully linked your Barracuda Backup Server, your Barracuda Cloud Storage service plan is activated. To ensure that you have a sufficient amount of offsite storage space at Barracuda Networks, it is important for you to verify that the plan size is the one you selected. View your Cloud Storage service plan size on the **STATUS** tab of the Barracuda Backup web interface.

Managing User Access

Use the **ADMIN > Users** page to administer users that have access to the Barracuda Backup web interface. This page has a link that takes you to Account/Support to add or remove users.

Related Articles
- Managing Your Account - Product Entitlements

Edit Users

Edit users from this page by selecting a user and clicking on the **Edit** (✏) icon. You can edit the following user options, all of which are specific to this service:

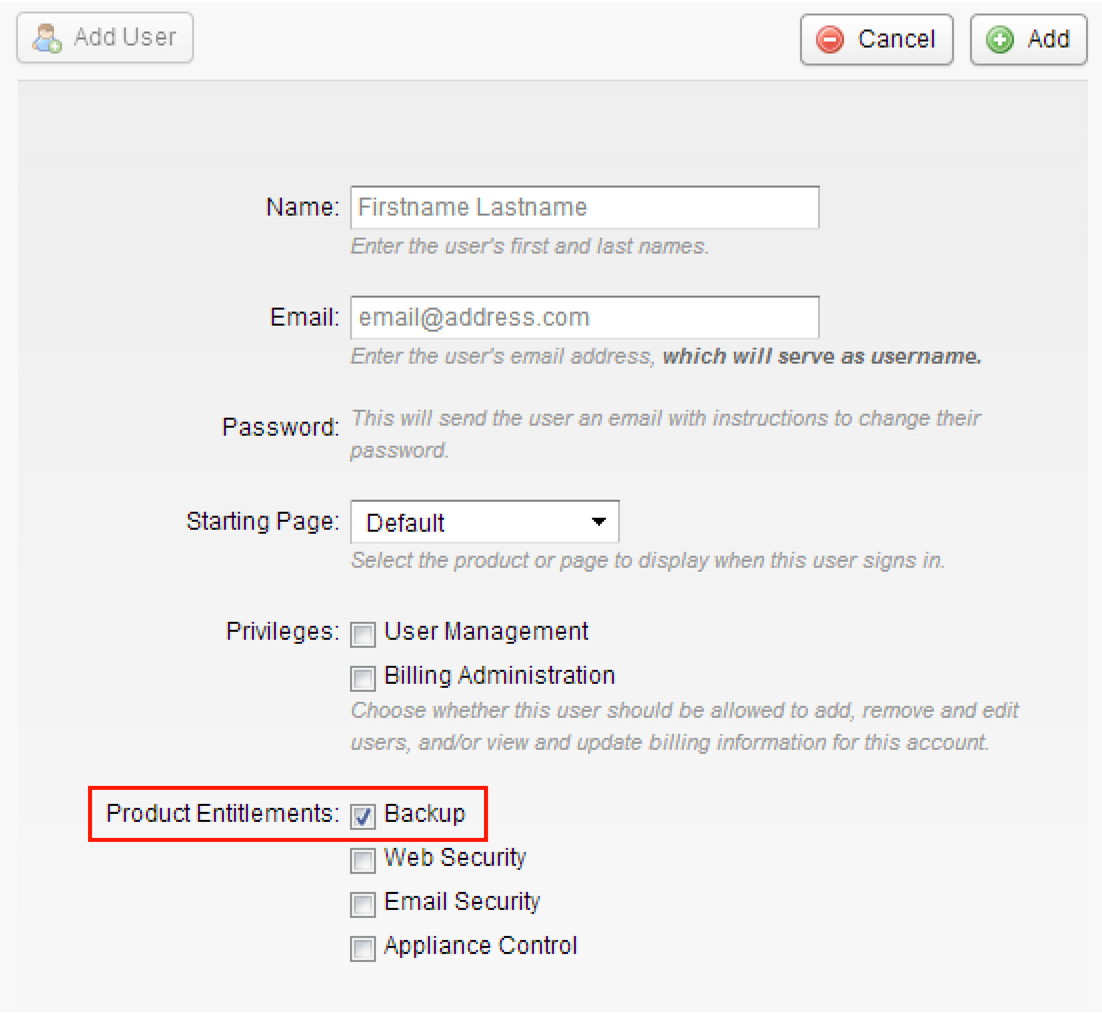
- Receive emails with backup reports, error condition alerts, or Barracuda Backup Server software update notices.
- Restrict access to the Barracuda Backup web interface to one or more IP addresses.
- Designate the user as an **Account Administrator**, **BBS Administrator**, or an **Operator**.
    - An *Account Administrator* can create new users and manage billing information, and has full access to all of the Barracuda Backup Servers associated with the account.
    - A *Barracuda Backup Server Administrator* has full access to specific Barracuda Backup Servers associated with the account including data restore. A Barracuda Backup Server Administrator cannot edit or view other user accounts.
    - An *Operator* cannot restore data or edit user accounts; operators are limited to viewing statistics and modifying backup configuration for selected Barracuda Backup Servers.

Product Entitlements

Use the following steps to add Barracuda Backup entitlements when you add a user to your Barracuda Networks account:

1. Log in to Barracuda Backup as the administrator, and go to the **ADMIN > Users** page.
2. Click **Add User**; the new user options display.
3. Enter the new username and email address; the user email address will be their username.
4. Select the **Starting Page** for this user upon log in from the following options:
    - **Default**
    - **Account**
    - **Community/Forum**
    - **Support**
5. In the **Privileges** section, you can optionally give the user the following privileges:
    - **User Management** - When selected, the user can add, remove, and edit users
    - **Billing Administration** - When selected, the user can view and update billing information for the account
    - In the **Product Entitlements** list, turn on **Backup**:

> ⓘ For details on adding additional subscribed to Barracuda Networks products and services, refer to connecting Barracuda Networks Products to Barracuda Cloud Control.



Name: Firstname Lastname
Enter the user's first and last names.

Email: email@address.com
Enter the user's email address, ***which will serve as username.***

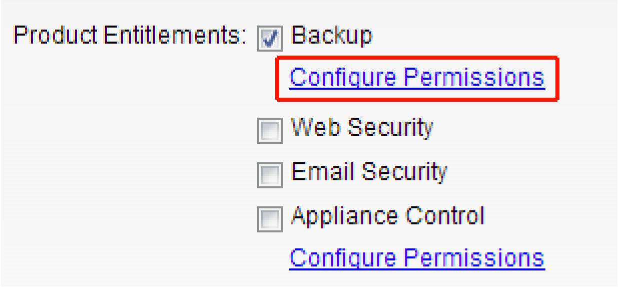
Password: *This will send the user an email with instructions to change their password.*

Starting Page: Default
Select the product or page to display when this user signs in.

Privileges: ☐ User Management
☐ Billing Administration
Choose whether this user should be allowed to add, remove and edit users, and/or view and update billing information for this account.

Product Entitlements: ☑ Backup
☐ Web Security
☐ Email Security
☐ Appliance Control

6. Click **Add** at the top of the page to add the user to Barracuda Backup; an email is then sent to the user prompting them to set their password.
7. Click on the username in the **Users** list; the user details display in the right pane. Under **Product Entitlements**, click **Configure Permissions**:



Product Entitlements: ☑ Backup
☐ Web Security
☐ Email Security
☐ Appliance Control

8. In the configuration page, you can set the following options:
    - Turn on the **Barracuda Email Notifications** for this user:
        - **Reports** - When turned on, a report is sent to this user for each backup job.
        - **Alerts** - When turned on, an alert is sent to this user if an error occurs during a backup job or if the Barracuda Backup Server goes offline.
        - **Notices** - when turned on, a notice is sent to this user when the Barracuda Backup Server software is updated.
    - **Authentication -** If you wish to restrict the IP address that this user is allowed to log in from, enter a value in the **IP Login Restrictions** field.
    - Specify user **Permissions:**
    - **Account Administrator** - User has full access to all Barracuda Backup Servers within the account.
    - **Barracuda Backup Server Administrator** - User has full access to all selected Barracuda Backup Servers; user does not have

    edit or view user accounts access. When selected, the **Backup Server Permissions** section displays:
        - **Select All Backup Servers** - When turned *On*, user has full access to all Barracuda Backup Servers within the account, when turned *Off*, a list of all connected devices display. Turn on the Barracuda Backup Servers to which this user is to have access.
    - **Operator** - User access is limited to viewing statistics and modifying backup configuration for selected Barracuda Backup SErvers. Operators cannot restore data or edit user accounts.
        - **Select All Backup Servers** - When turned *On*, user has *Operator* access privileges to all Barracuda Backup Servers within the account, when turned *Off*, a list of all connected devices displays. Turn on the Barracuda Backup Servers to which this user is to have *Operator* access.
9. Click **Save** at the top of the page to save the Backup configuration settings for the selected user.

Email Notifications Page

Notification Types

Specify the type of email notification for each user:

- **Reports** - When selected, an email notification is sent for each backup job.
- **Alerts** - When selected, an email notification is sent if a backup job has errors or if your Barracuda Backup Server is offline.
- **Notices** - When selected, an email notification is sent when your Barracuda Backup Server software is updated.

Managing Email Notifications

Use the **ADMIN > Users** page to specify whether a user is to receive email notifications. Edit users from this page by selecting a user and clicking on the **Edit** graphic. You can specify whether a user is to receive one or more of the following types of emails:

- Backup reports saying that a scheduled back up was run
- Alerts for conditions such as:
    - A Barracuda Backup Server is offline or has come online
    - A Barracuda Backup Server has not been able to communicate with Barracuda Cloud Storage (check for Internet problems)
    - A Barracuda Backup Server appliance, such as a RAID volume or HD hardware, fails
    - A watched file rule condition has been met (firmware version 5.1 and earlier only)
    - An error has occurred in a backup
    - An error situation returned to normal and no (further) action is required
    - You have reached the limit on your Barracuda Cloud Storage subscription plan size
- Notices of Barracuda Backup Server software updates

Use the **ADMIN > Email Notifications** page to specify email addresses of non-users that are to receive an email when a report, alert, or notice generates. This page allows you to specify any email address (in some cases, your reseller), not only the email address of a user associated with your account. You can also see the users that are receiving any type of email notification, and edit those users in a similar way to the **ADMIN > Users** page.

Display Groups Page

Display Groups

If you have multiple Barracuda Backup Servers, you can manage them through display groups:

1. Log in to Barracuda Backup, and go to the **ADMIN > Display Groups** page.
2. All display groups active on your account display in the **Current Display Groups** section.
3. To add a new display group, enter a name for the group of devices, and click **Add**. For example, if you want to group all Barracuda Backup by location, you might create groups by geographic location: Engineering - Asia, Engineering - US, Engineering - Europe.
4. The display group name appears in the **Current Display Groups** section.
5. To remove a display group, click **Remove** following the name of the group you want to remove; click **OK** to confirm you want to remove the group.

    > ⓘ If you delete a display group that contains devices, those devices are moved to the default group.

Add a Barracuda Backup Server to the Group

Once you create display groups, you can add a Barracuda Backup Server to the group using the following steps:

1. In the left pane, select the appropriate Barracuda Backup, and go to the **SYSTEM > BBS Settings** page.
2. In the **Backup Server Display Group** section, choose from the **Current Display Group** drop-down list, select the display group name.
3. To add or remove display groups, click **Manage your display groups** to go to the **ADMIN > Display Groups** page.
4. Click **Save**.

Documentation Page

Access the Barracuda Networks Solutions Knowledgebase and Barracuda TechLibrary articles.

Link a Barracuda Backup Server Page

Use this page to set up your Barracuda Backup Server. The Barracuda Backup Server must be linked online before backups can be initiated. See the following articles for details on linking and unlinking a Barracuda Backup Server:

- Link a Barracuda Backup Server as a User or Reseller
- Unlink a Barracuda Backup Server

How to Link a Barracuda Backup Server as a User or Reseller

This article refers to Barracuda Backup firmware version 3.0 or higher.

In this article:

- Initial Set Up
- Link a Barracuda Backup Server to your Account
- Link a Barracuda Backup Server as a Reseller

Related Articles
• Unlink a Barracuda Backup Server

Initial Set Up

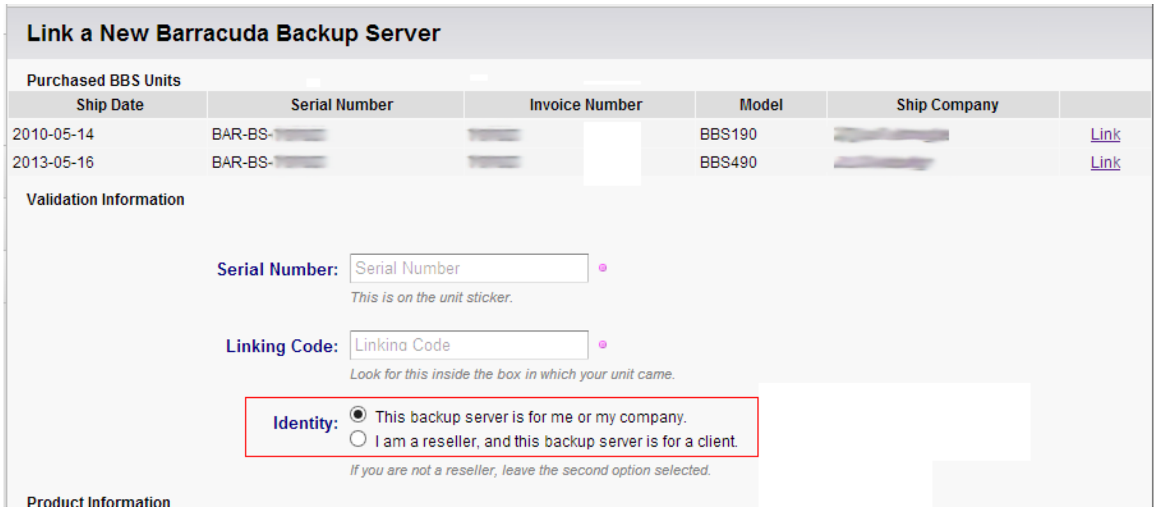
The Barracuda Backup Server must be linked online before backups can be initiated. You must have billing information (credit card recommended) to complete the linking process.

1. Go to http://login.barracuda.com, and log in.
2. Once logged in, click **Backup Service** in the left pane. If this is your first time linking a Barracuda Backup Server, click **Start Backup Service Setup**; otherwise, click **Link a Barracuda Backup Server** in the left pane.
3. On the **Validation** page, enter the serial number and the linking code for the Barracuda Backup Server from the sticker included on the Barracuda Backup Server Quick Start Guide included with the appliance.
4. In the **Identity** section, you are presented with two options. Your selection determines how the unit is linked to an account:
    - This backup server is for me or my company
    - I am a reseller and this backup server is for a client

Link a Barracuda Backup Server to your Account

Once you complete the steps in the **Initial Set Up** section, you can link the appliance for yourself or your company:

1. In the **Identity** section, select **This backup server is for me or my company**:



Link a New Barracuda Backup Server

Purchased BBS Units

Ship Date	Serial Number	Invoice Number	Model	Ship Company	
2010-05-14	BAR-BS-[redacted]	[redacted]	BBS190	[redacted]	Link
2013-05-16	BAR-BS-[redacted]	[redacted]	BBS490	[redacted]	Link

Validation Information

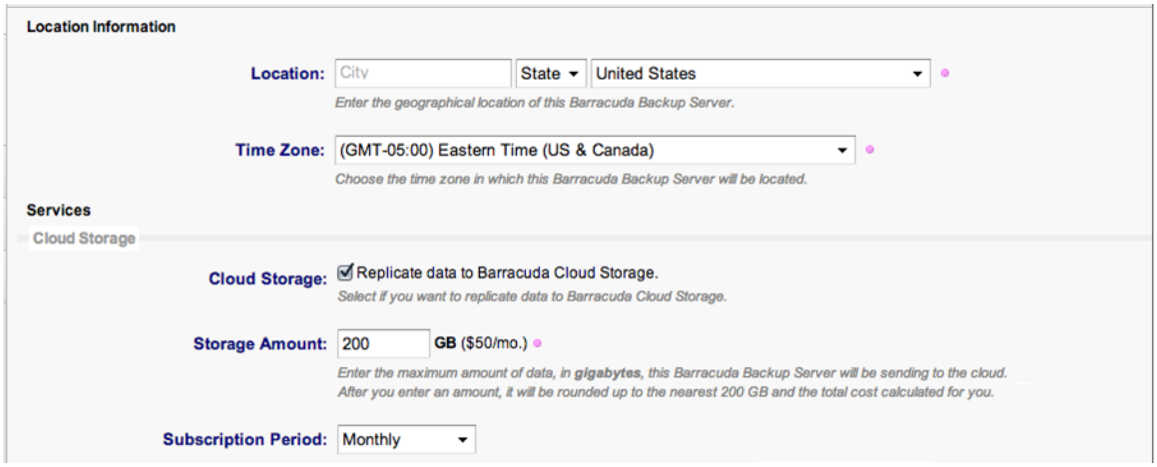
Serial Number: Serial Number
This is on the unit sticker.

Linking Code: Linking Code
Look for this inside the box in which your unit came.

Identity: ● This backup server is for me or my company.
○ I am a reseller, and this backup server is for a client.
If you are not a reseller, leave the second option selected.

Product Information

2. Click **Continue**. In the next page, enter the physical location and time zone details, and choose a Cloud Storage subscription plan if you intend to replicate data to Barracuda Cloud Storage; no Cloud Storage subscription is required for site-to-site replication.



Location Information

Location: City | State | United States
Enter the geographical location of this Barracuda Backup Server.

Time Zone: (GMT-05:00) Eastern Time (US & Canada)
Choose the time zone in which this Barracuda Backup Server will be located.

Services

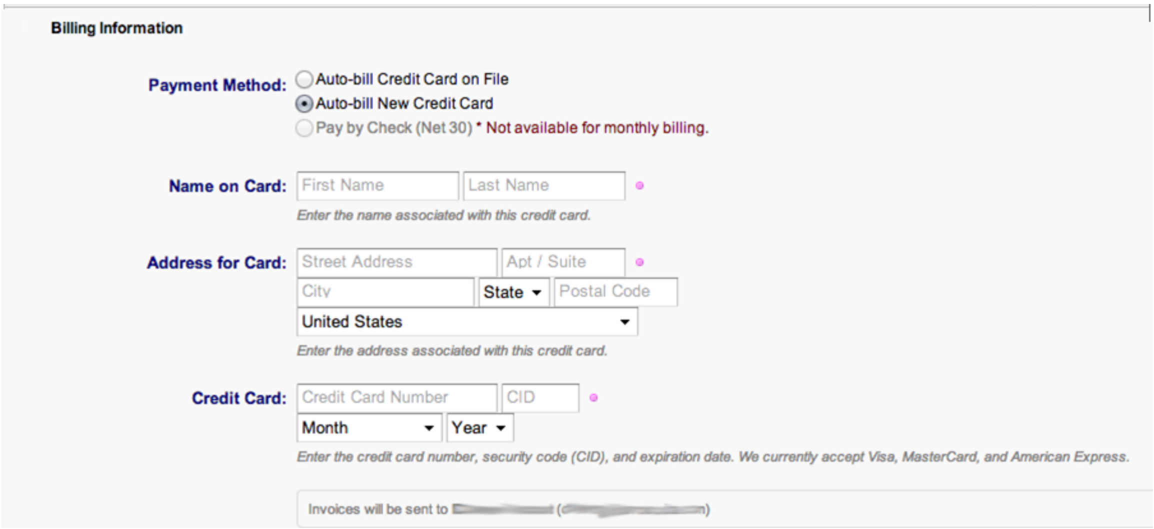
Cloud Storage

Cloud Storage: ☑ Replicate data to Barracuda Cloud Storage.
Select if you want to replicate data to Barracuda Cloud Storage.

Storage Amount: 200 **GB** ($50/mo.)
*Enter the maximum amount of data, in **gigabytes**, this Barracuda Backup Server will be sending to the cloud. After you enter an amount, it will be rounded up to the nearest 200 GB and the total cost calculated for you.*

Subscription Period: Monthly

3. Click **Continue**. In the next page, enter the billing information:



Billing Information

Payment Method: ○ Auto-bill Credit Card on File
● Auto-bill New Credit Card
○ Pay by Check (Net 30) * Not available for monthly billing.

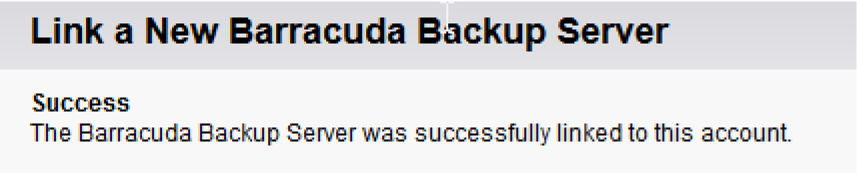
Name on Card: First Name | Last Name
Enter the name associated with this credit card.

Address for Card: Street Address | Apt / Suite
City | State | Postal Code
United States
Enter the address associated with this credit card.

Credit Card: Credit Card Number | CID
Month | Year
Enter the credit card number, security code (CID), and expiration date. We currently accept Visa, MasterCard, and American Express.

Invoices will be sent to [redacted] ([redacted])

4. Click **Link Barracuda Backup Server** to link the unit to the account you logged into in the **Initial Set Up** section*:*



Link a New Barracuda Backup Server

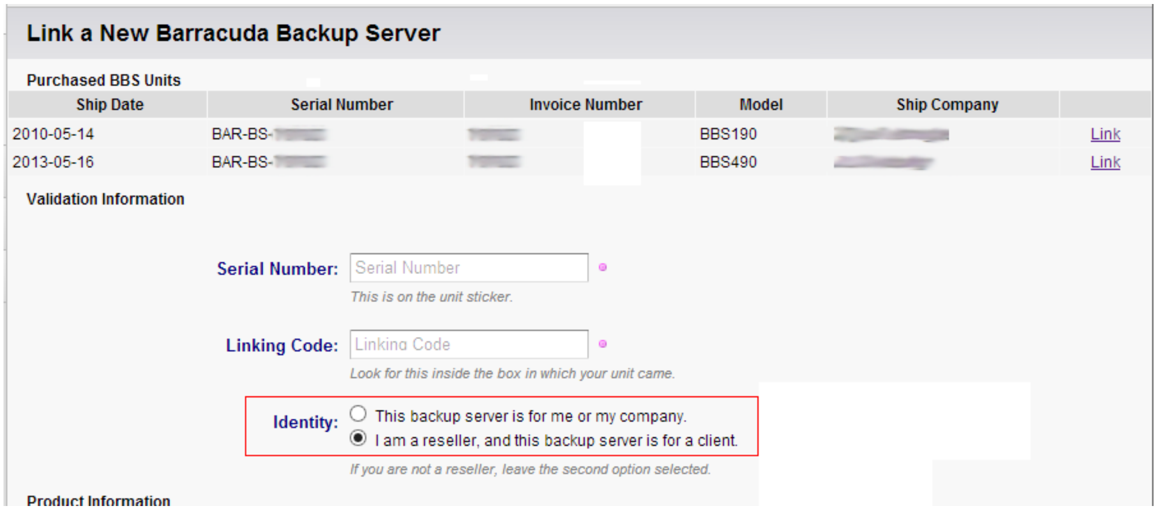
Success
The Barracuda Backup Server was successfully linked to this account.

5. Once the unit is linked, the firmware is updated and the appliance reboots. When the unit comes back online you must log out and then log back in to the user interface to clear any cached pages.
6. Data sources can now be set up on the Barracuda Backup Server.

Link a Barracuda Backup Server as a Reseller

Once you complete the steps in the **Initial Set Up** section, you can link the client appliance as a reseller:

1. In the **Identity** section, select **I am a reseller and this backup server is for a client**:



Link a New Barracuda Backup Server

Purchased BBS Units

Ship Date	Serial Number	Invoice Number	Model	Ship Company	
2010-05-14	BAR-BS-[redacted]	[redacted]	BBS190	[redacted]	Link
2013-05-16	BAR-BS-[redacted]	[redacted]	BBS490	[redacted]	Link

Validation Information

Serial Number: Serial Number
This is on the unit sticker.

Linking Code: Linking Code
Look for this inside the box in which your unit came.

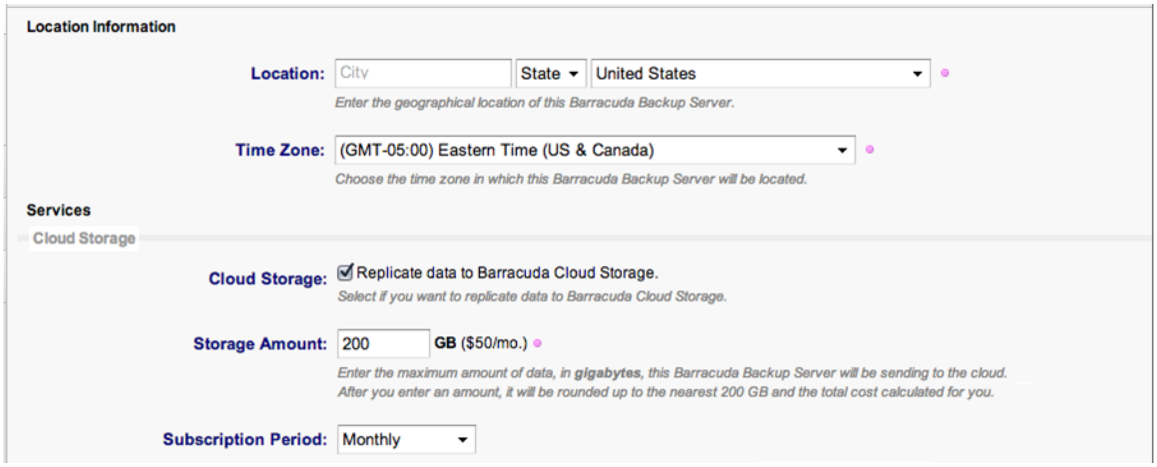
Identity: ○ This backup server is for me or my company.
● I am a reseller, and this backup server is for a client.
If you are not a reseller, leave the second option selected.

Product Information

2. When selected, an additional set of dialog boxes display where you add the end-user information. Click **Continue**.

> The details added in this set of dialog boxes are used to create an account to which the unit is linked, and to which the reseller is then granted access. This allows a reseller to *manage* multiple Barracuda Backup Servers from one central location in the UI, while giving the end-customer access to their individual appliances. Note that a reseller can determine whether to have access to the appliance once it is linked.

3. In the next page, enter the physical location and time zone details, and choose a Cloud Storage subscription plan if your client intends to replicate data to Barracuda Cloud Storage; no Cloud Storage subscription is required for site-to-site replication:



Location Information

Location: City | State | United States
Enter the geographical location of this Barracuda Backup Server.

Time Zone: (GMT-05:00) Eastern Time (US & Canada)
Choose the time zone in which this Barracuda Backup Server will be located.

Services

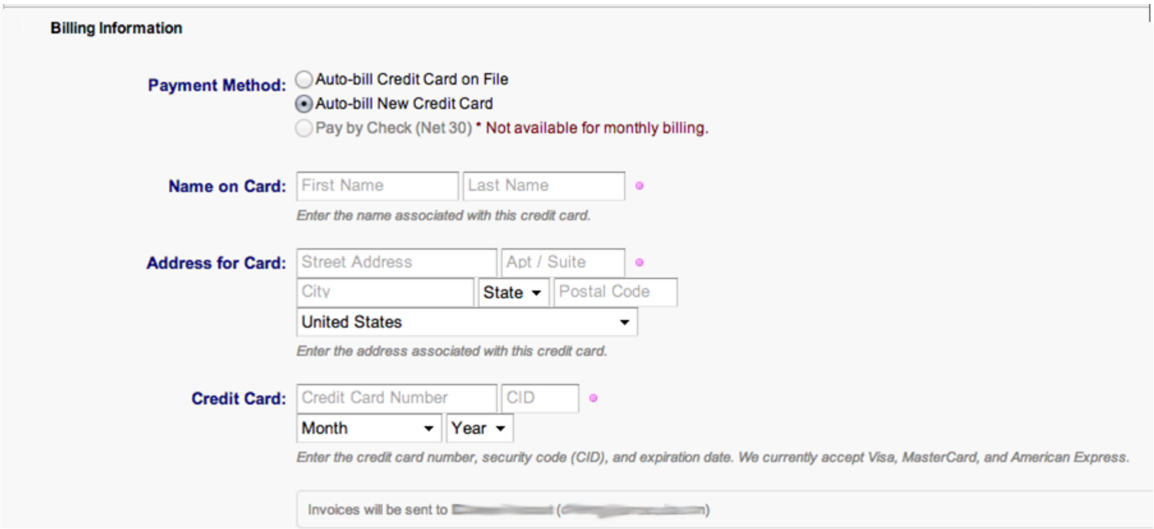
Cloud Storage

Cloud Storage: ☑ Replicate data to Barracuda Cloud Storage.
Select if you want to replicate data to Barracuda Cloud Storage.

Storage Amount: 200 GB ($50/mo.)
*Enter the maximum amount of data, in **gigabytes**, this Barracuda Backup Server will be sending to the cloud. After you enter an amount, it will be rounded up to the nearest 200 GB and the total cost calculated for you.*

Subscription Period: Monthly

4. Click **Continue**. In the next page, enter the client's billing information:



Billing Information

Payment Method: ○ Auto-bill Credit Card on File
● Auto-bill New Credit Card
○ Pay by Check (Net 30) * Not available for monthly billing.

Name on Card: First Name | Last Name
Enter the name associated with this credit card.

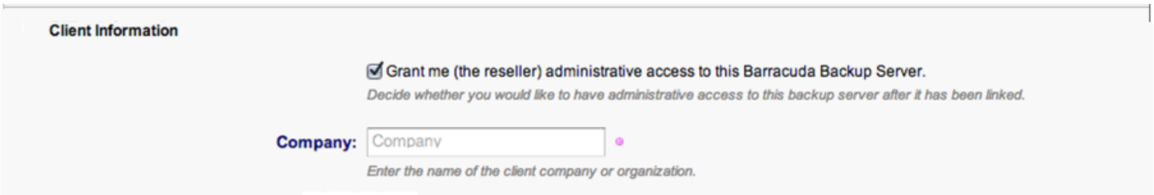
Address for Card: Street Address | Apt / Suite
City | State | Postal Code
United States
Enter the address associated with this credit card.

Credit Card: Credit Card Number | CID
Month | Year
Enter the credit card number, security code (CID), and expiration date. We currently accept Visa, MasterCard, and American Express.

Invoices will be sent to [redacted] ([redacted])

5. Click **Continue**. In the **Client Information** page, specify whether you want to have access to the unit after it has been linked, and enter the name of the client organization:

> ⚠ If you turn **Grant me (the reseller) administrative access to this Barracuda Backup Server** off, the only way to manage the linked unit is through the end-user (client) credentials.

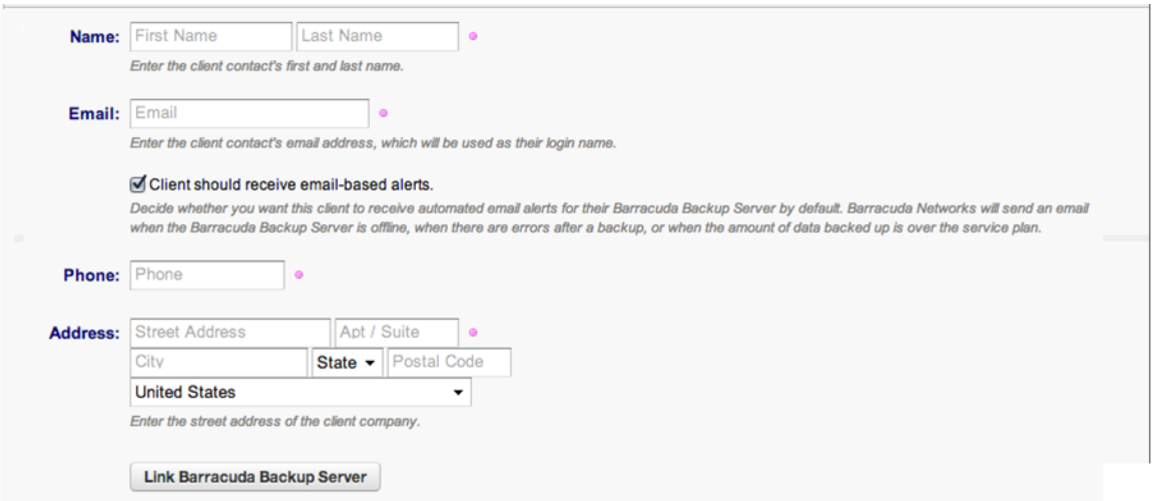


Client Information

☑ Grant me (the reseller) administrative access to this Barracuda Backup Server.
Decide whether you would like to have administrative access to this backup server after it has been linked.

Company: Company
Enter the name of the client company or organization.

6. Enter the client contact details:



Name: First Name | Last Name
Enter the client contact's first and last name.

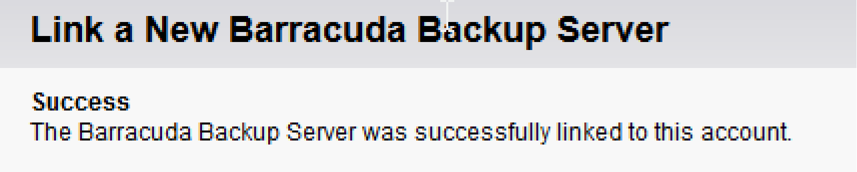
Email: Email
Enter the client contact's email address, which will be used as their login name.

☑ Client should receive email-based alerts.
Decide whether you want this client to receive automated email alerts for their Barracuda Backup Server by default. Barracuda Networks will send an email when the Barracuda Backup Server is offline, when there are errors after a backup, or when the amount of data backed up is over the service plan.

Phone: Phone

Address: Street Address | Apt / Suite
City | State | Postal Code
United States
Enter the street address of the client company.

7. Click **Link Barracuda Backup Server:**



Link a New Barracuda Backup Server

Success
The Barracuda Backup Server was successfully linked to this account.

8. Once the unit is linked, the firmware is updated and the appliance reboots. When the unit comes back online you must log out and then log back in to the user interface to clear any cached pages.
9. Data sources can now be set up on the Barracuda Backup Server.

Security

In this Section

- Backup Security and Site-to-Site Replication
- Barracuda Cloud Storage Standards and Protection
- Policy-Based Security
- How to Secure Your Barracuda Backup Server

Backup Security and Site-to-Site Replication

When using a site-to-site deployment, you need to ensure the physical security of the remote Barracuda Backup Servers. Typically the Barracuda Backup Servers are kept behind corporate firewalls and communicate with each other using a VPN tunnel.

Barracuda Cloud Storage Standards and Protection

In this article:

- Facility Standards
- Storage
- Oversight
- Verify Service Plan Size

Related Articles
- Barracuda Cloud Control

Facility Standards

Barracuda Networks leases space in a number of Tier 3 and 4 facilities across the world. Each of these storage locations is equipped with:

- Controlled access systems requiring key-card authentication and physical check-in
- Video-monitored access points
- Intrusion alarms
- Locking cabinets
- Climate control systems
- Waterless fire suppressant systems
- Redundant power (generator backup, UPS, no single point of failure)
- Redundant Internet connectivity

The Barracuda Cloud Storage infrastructure boasts high-quality RAID hardware with hot-spare drives in every file server, and near instant data mirroring over high-speed fiber connections between the storage locations.

Storage

In the United States, data is transmitted from Barracuda Backup Servers to one data center, and then replicated to another. The process of replicating data begins immediately after it is copied from a Barracuda Backup Server, and runs continuously. Data in Barracuda Cloud Storage is stored in parts, and no single computer in the storage system has all the parts required to reconstruct data. Each of these computer systems communicates in unison to deliver restored data securely. This diverse storage system serves to further strengthen the physical security of your data.

With this architecture, Barracuda Networks equipment can maintain up to three distinct copies of your data which can be stored in three geographically separate locations.

Oversight

Access to Barracuda Backup Servers is limited to approved Barracuda Networks employees on an 'as needed' basis. Employee activity is logged, and all logs are archived to an independent storage device.

Verify Service Plan Size

After you have successfully linked your Barracuda Backup Server, your Barracuda Cloud Storage service plan is activated. To ensure that you have a sufficient amount of offsite storage space at Barracuda Networks, it is important for you to verify that the plan size is the one you selected. View your Barracuda Cloud Storage service plan size on the **STATUS** tab of the Barracuda Backup web interface.

Policy-Based Security

Data retention policies allow you to specify the retention of selected files or broader data based on daily, weekly, monthly or annual time intervals. You can create multiple retention policies for different types of data:

- Files
- Data backed up by the Barracuda Backup Agent (Exchange, SQL, system state)
- Email messages

Retention policies are the only way to purge data; data cannot be deleted directly by a user.

How to Secure Your Barracuda Backup Server

The Barracuda Backup Server is deployed behind your corporate firewall, and is protected by the same security as your primary data sources.

In this article:

- Communication and Configuration
- Data Transmission and Storage
- Management Access
- Encryption

Related Articles

- Barracuda Cloud Storage Standards and Protection

Communication and Configuration

Administration and backup configuration that is set using the Barracuda Backup web interface is sent to the Barracuda Backup Server via a 256-bit encrypted VPN tunnel. The Barracuda Backup Server uses HTTPS port 1194 to send status updates to Barracuda Backup. Data transfers are initiated by the Barracuda Backup Server rather than by Barracuda Cloud Storage or a remote Barracuda Backup Server.

Data Transmission and Storage

Data transferred between your network and Barracuda Cloud Storage, or between your network and a remote Barracuda Backup Server, is always encrypted. File parts are AES 256-bit symmetrically encrypted before they are stored, and they remain encrypted until a restore is requested.

Management Access

- **Monitor Activity** - You can check the user activity page periodically for authentication attempts, changes to settings, and updates to account information. Go to the **ADMIN > User Activity Reports** page to see all activity for an account, including logins and when a user has enabled or disabled replication.
- **Restrict Logins by IP Address** - You can restrict access to Barracuda Backup to one or more IP addresses. On the **ADMIN > Users** page, click the **Edit** graphic (✏) to edit a user account; enter an IP address or a range.
- **Secure Network Access** - HTTPS is always used for secure web browser communication with Barracuda Backup.

Encryption

Data transfers from the local Barracuda Backup Server to a receiving Barracuda Backup Server are always encrypted. Data is stored compressed and encrypted at rest on the receiving Barracuda Backup Server; the local Barracuda Backup Server does not store in an encrypted or compressed state. The most aggressive combination of symmetrical and asymmetrical encryption in the industry keeps your data stored in a format that nobody but you can access. The United States government recently approved 192-bit AES encryption as the preferred method for protecting top-secret information. The Barracuda Backup solution starts with even higher 256-bit AES encryption.

In addition, Barracuda Networks has developed a proprietary advanced digital cataloging system that breaks down your data into small pieces and tracks the changes of these parts over time, and strips the original meta identifiers from your files.

As data is transmitted to the remote Barracuda Backup Server, your symmetrically-encrypted data parts are compressed and sent over your Internet connection with an asymmetrically-encrypted key.

System Management

In this Section

- Barracuda Backup Replacement and Data Migration
- Replacing a Failed Barracuda Backup Server
- How to Shut Down a Barracuda Backup Server
- How to Wipe a Barracuda Backup Server
- Barracuda Backup Server Panel Indicators, Ports, and Connectors
- Barracuda Backup Server Hardware Specifications
- How to Physically Install the Barracuda Backup Server

Related Articles

- How to Link a Barracuda Backup Server
- How to Unlink a Barracuda Backup Server
- Firmware Page
- BBS Settings Page
- Software Downloads Page

Barracuda Backup Replacement and Data Migration

> This article refers to all Barracuda Backup firmware versions.
>
> If you have any questions or concerns regarding your Barracuda Backup Replacement, contact Barracuda Networks Technical Support.

In this article:

- Setting Up the New Barracuda Backup Server
- Data Migration Options
  - Option 1. Pull Data from the Cloud
  - Option 2. Pull Data from an Existing Barracuda Backup Server
  - Option 3. Use an Existing Barracuda Backup Server Configuration
  - Option 4. Set Up a New Barracuda Backup Server from Scratch

Setting Up the New Barracuda Backup Server

Before you can replace a device and migrate the data, you must first install and configure the new Barracuda Backup Server. Use Step 1 and Step 2 in the Getting Started section of this library, or refer to the Barracuda Backup Quick Start Guide available for download on the Barracuda Backup Overview page.

Data Migration Options

Select the data migration option that best suits your deployment.

Option 1. Pull Data from the Cloud

If you elect to pull the data from the cloud, Barracuda Networks uses the following procedure to complete your request:

1. Once the new unit is linked, Barracuda Networks connects to the new device and begins wiping the metadata in the database ensuring the unit is completely clean of any data.
2. Barracuda Networks then pulls the metadata associated with all binary data (your backed-up data).

> The *metadata* is a description of the data, whereas the *binary data* is comprised of your actual files.

3. As the metadata is downloaded, it is inserted into the database tables on the new device. Depending on the amount of metadata to be pulled, this process may take 24 or more hours to complete.
4. Once the metadata download is complete, backups are enabled on the new device, and the binary data is then pulled from the cloud. The process of pulling the binary data from the cloud can take 24 hours or more depending on the amount of data to be retrieved.
5. You will receive a notification at the time of backups start and the binary data begins to be pulled.

> At this point you can make any changes to the configuration via the web interface; the device is now at full capability.

6. Once the initial binary data pull is complete, a final check is run with the cloud to ensure data integrity and to verify that all data is present and accounted for. Once verification is complete, the data migration as a whole is finished.
7. You will receive a notification indicating the process is complete.

Option 2. Pull Data from an Existing Barracuda Backup Server

If you have elected to pull the data from your existing Barracuda Backup Server, confirm the following:

- Both units are on the same LAN/subnet, and
- Both units are linked to a Barracuda Networks Account

1. Once the new device has been linked to the existing Barracuda Backup Server, Barracuda Networks begins prepping the old device for the migration including:
    - Shutting down all dependent functions of the old device
    - Dumping the metadata tables from the databases on the old unit in order to pull them across and import them into the new device.
2. Once prepping is complete, Barracuda Networks begins the actual data migration by importing the metadata tables from the old device to the new unit.
3. Once the import is complete, the binary data is synchronized across to the new unit. AT this point, backups are enabled on the new device and a backup is run on all data sources.

> Running a backup on all data sources assists in populating the new device with the synchronized data. By backing up the data sources, those data parts that already exist are skipped over, thus reducing the time it takes to complete the process.

4. You will receive a notification alerting you that the backup process has begun on the new device and that data is syncing.
5. Once the initial binary data pull is complete, a final check is run with the cloud to ensure data integrity and to verify that all data is present and accounted for. Once verification is complete, the data migration as a whole is finished.
6. You will receive a notification indicating the process is complete.

Option 3. Use an Existing Barracuda Backup Server Configuration

You can set up and configure a new Barracuda Backup Server with an existing configuration, data sources, retention policies, and all other aspects of backup.barracuda.com.

This is the fastest type of migration because you are not migrating large amounts of data.

1. Once the new device is linked, Barracuda Networks pulls the configuration from the cloud.
2. You will receive a notification indicating the process is complete.

Option 4. Set Up a New Barracuda Backup Server from Scratch

You can set up and configure a new Barracuda Backup Server without utilizing an existing configuration. With this option, you must configure the new device from scratch as it is treated as a brand new unit. For step-by-step instructions on setting up backups, refer to Data Backup Tasks in the Getting Started section.

Replacing a Failed Barracuda Backup Server

Related Articles
- How Barracuda Networks Manages Returned Device Drives

Barracuda Networks Technical Support
Before you replace your Barracuda Backup Server, contact Barracuda Networks Technical Support to try to resolve the problem.

Troubleshooting

Use the articles in the Troubleshooting and Error Messages section of this TechLibrary to help resolve issues encountered on your system.

Instant Replacement Service

In the event that a Barracuda Backup Server fails and you cannot resolve the issue, customers that have purchased the Instant Replacement service can contact Barracuda Networks Technical Support to arrange for a new unit to be shipped out within 24 hours.

After receiving the new system, ship the old Barracuda Backup Server back to Barracuda Networks at the address below with the Return Material Authorization (RMA) number clearly marked on the package; Barracuda Networks Technical Support can provide details on the best way to return the unit:

> Barracuda Networks, Inc.
> 3175 S. Winchester Blvd
> Campbell, CA   95008
>
> attn: RMA # *<your RMA number>*

How to Shut Down a Barracuda Backup Server

You can remotely reboot or shut down a Barracuda Backup Server by logging into its local web interface. Type the IP address of the Barracuda Backup Server in a web browser and log in using your Barracuda Networks account.

You can also perform a safe shutdown of a Barracuda Backup Server by pressing the **POWER** button on the front of the device. This issues a shutdown command to all system and service processes before the device powers down.

Caution
Do not push the **POWER** button for more than a couple of seconds. Holding it for five seconds or longer causes an immediate hard shutdown. This interrupts running processes and the Barracuda Backup Server powers off before unmounting the file system.

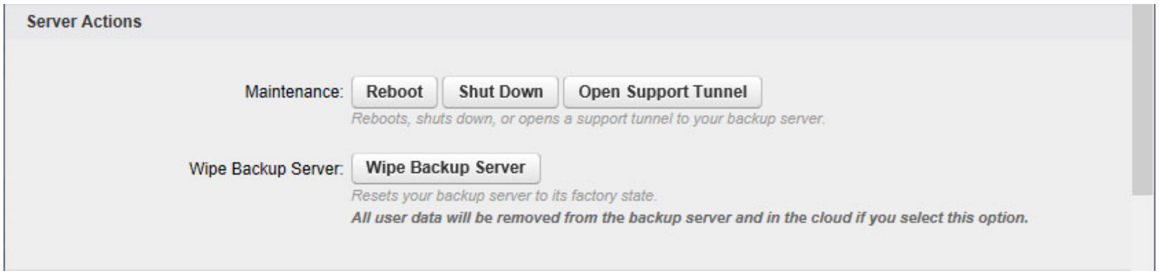
How to Wipe a Barracuda Backup Server

This article refers to Barracuda Backup firmware version 3.0 or higher.

Wiping a Barracuda Backup Server unlinks it from your account and puts all data and configuration information into a queue to be purged from Barracuda Cloud Storage. The wipe feature also deletes the contents of the local databases on the Barracuda Backup Server, moves the binary data on the Barracuda Backup Server into a temporary storage location on the system, and then shuts it down. The next time the Barracuda Backup Server is booted the binary data that has been moved is deleted.

Use the following steps to wipe a Barracuda Backup Server to unlilnk it from your account:

1. Enter the Barracuda Backup Server IP address to log in to the local web interface.
2. Go to the **STATUS** page, and in the **Server Actions** section, click **Wipe Backup Server**:



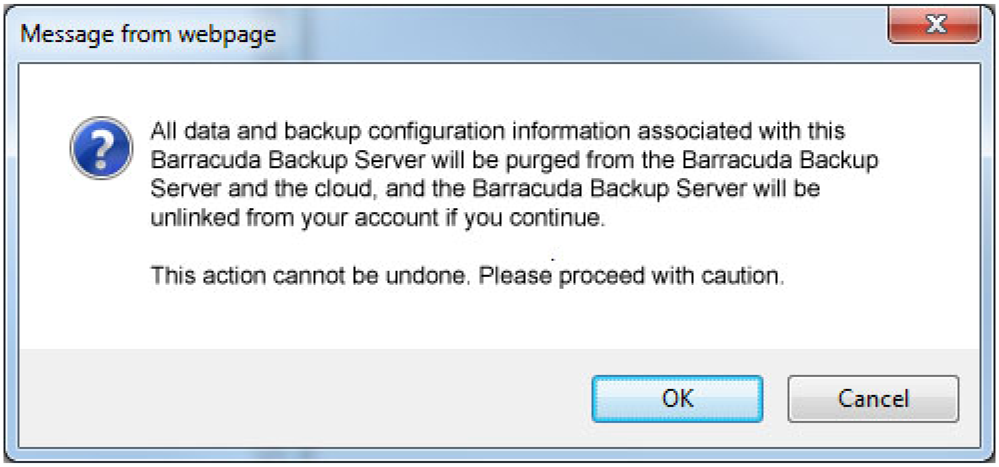
Server Actions
Maintenance:
Reboot
Shut Down
Open Support Tunnel
Wipe Backup Server:
Wipe Backup Server

Reboots, shuts down, or opens a support tunnel to your backup server.

Resets your backup server to its factory state.

All user data will be removed from the backup server and in the cloud if you select this option.

3. The message **Wipe Started Successfully** displays in the web interface. Once the unlinking process is in progress, a warning message displays:

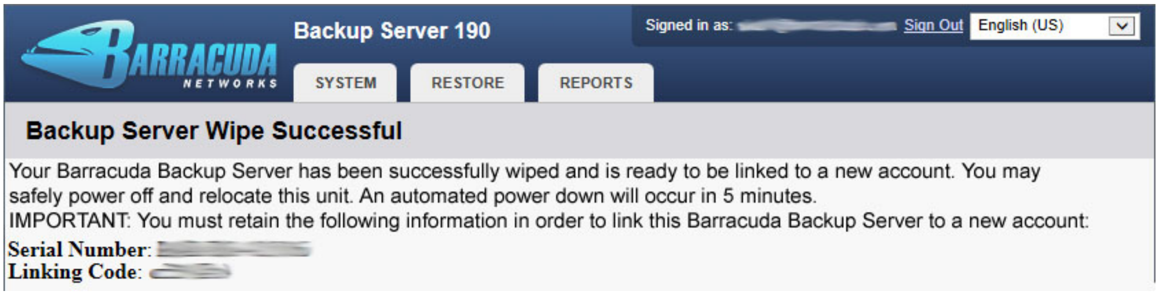


Message from webpage
OK
Cancel

All data and backup configuration information associated with this Barracuda Backup Server will be purged from the Barracuda Backup Server and the cloud, and the Barracuda Backup Server will be unlinked from your account if you continue.

This action cannot be undone. Please proceed with caution.

4. Click **OK** to complete the unlinking process. Once the Barracuda Backup Server is unlinked from the account, the **Backup Server Wipe Successful** page displays, including the Serial Number and Linking Code:



Backup Server 190
Signed in as: [redacted]
Sign Out
English (US)
SYSTEM
RESTORE
REPORTS

Backup Server Wipe Successful

Your Barracuda Backup Server has been successfully wiped and is ready to be linked to a new account. You may safely power off and relocate this unit. An automated power down will occur in 5 minutes.

IMPORTANT: You must retain the following information in order to link this Barracuda Backup Server to a new account:

Serial Number: [redacted]
Linking Code: [redacted]

5. Make note of the serial number and linking code. You can now link the Barracuda Backup Server to a new account. For details, see How to Link a Barracuda Backup Server as a User or Reseller.

Barracuda Backup Server Panel Indicators, Ports, and Connectors

This article refers to Barracuda Backup firmware version 5.0 and higher.

In this article:

- Barracuda Backup Server Model 190 and 390
- Barracuda Backup Server Model 490 and 690
- Barracuda Backup Server 890, 891, 892, 990, and 991
- Barracuda Backup Server 1090 and 1091

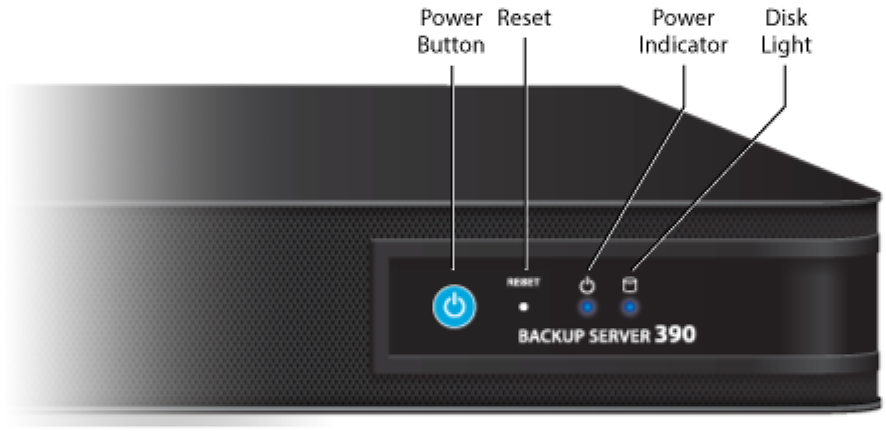
Related Articles

- Barracuda Backup Server Hardware Specifications
- How to Physically Install the Barracuda Backup Server

Barracuda Backup Server Model 190 and 390

The following figure illustrates the Barracuda Backup power and disk activity indicator lights for models 190 and 390.

Model 190 and 390 Front Panel


Power Button
Reset
Power Indicator
Disk Light
RESET
BACKUP SERVER 390

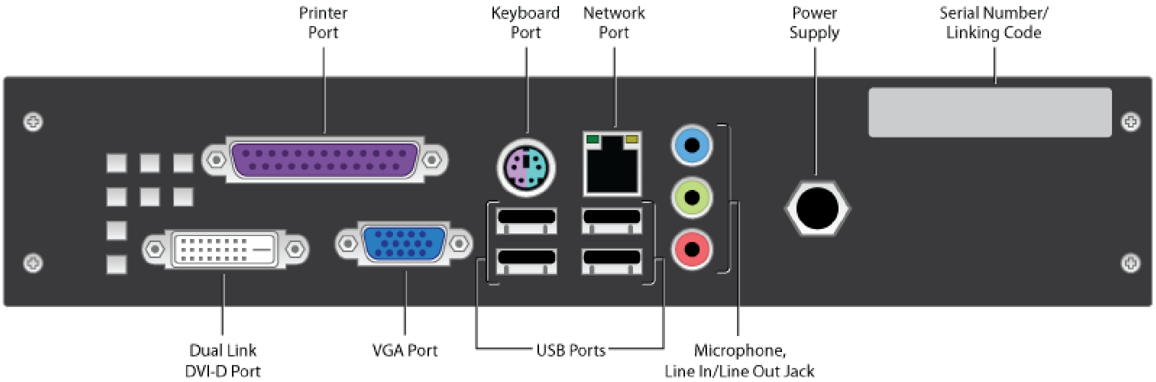
The following table describes the Barracuda Backup front panel power and disk activity indicator lights for models 190 and 390.

Model 190 and 390 Front Panel Component Description

Component Name	Description
Power Button	Push to power on the Barracuda Backup Server, tap to safely reset the Barracuda Backup Server.
Reset Button	Push for 5 seconds to reset the Barracuda Backup Server.
Power Light	Displays a solid green light when the system is powered on.
Disk Light	Displays a solid green light and blinks during disk activity.

The following figure illustrates the Barracuda Backup rear panel ports and connectors for model 190.

Model 190 Rear Panel


Printer Port
Keyboard Port
Network Port
Power Supply
Serial Number/ Linking Code
Dual Link DVI-D Port
VGA Port
USB Ports
Microphone, Line In/Line Out Jack

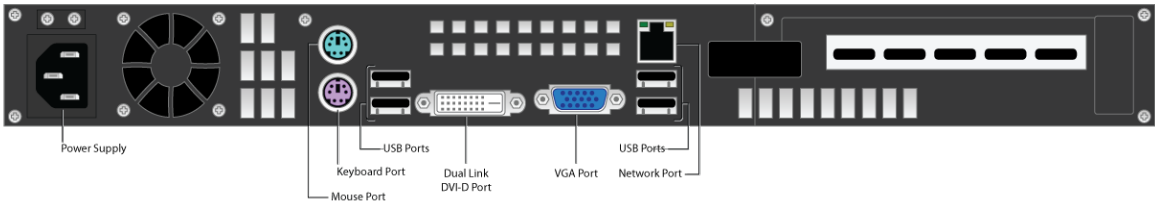
The following table describes the Barracuda Backup power and disk activity indicator lights for model 190.

Model 190 Rear Panel Port and Connector Description

Port/Connector Name	Details
Dual Link DVI-D Port	*Optional*. Digital monitor connection.
Printer Port	*Optional.* Printer connection.
VGA Port	*Recommended*. Video graphics array (VGA) monitor connection.
Keyboard Port	*Optional*. PS2 keyboard connection.
Network Port	Network port.
USB Ports (4)	*Optional.* USB device connection.
Microphone	*Optional.* Microphone line-in connection.
Line In/Line Out Jack	*Optional.* Audio input/output connections.
Power Supply	Power supply input.
Serial Number/Linking Code	Use the linking code to initiate Barracuda Backup Server backups.

The following figure illustrates the Barracuda Backup rear panel ports and connectors for model 390.

Model 390 Rear Panel



The following table describes the Barracuda Backup rear panel ports and connectors for model 390.

Model 390 Rear Panel Port and Connector Description

Port/Connector Name	Details
Power Supply	Power supply input.
Mouse Port	*Optional*. Mouse port.
Keyboard Port	*Optional* . PS2 keyboard connection.
Dual Link DVI-D Port	*Optional*. Digital monitor connection.
VGA Port	*Recommended*. Video graphics array (VGA) monitor connection.
Network Port	Network port.
USB Ports (4)	*Optional.* USB device connection.

Barracuda Backup Server Model 490 and 690

The following table describes the front panel indicator lights for models 490 and 690.

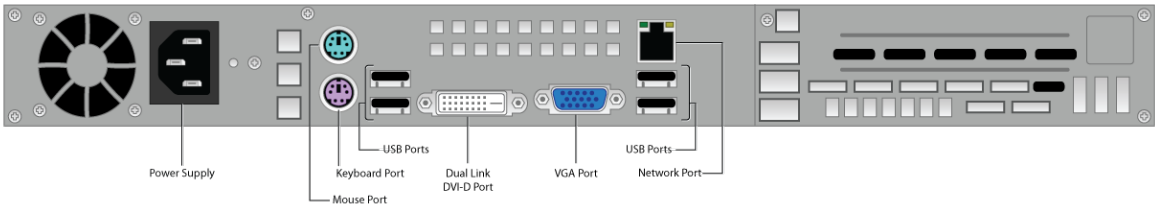
Model 490 and 690 Front Panel Component Description

Component Name	Description
Reserved	*Reserved for future use.*

Network Activity (2)	Blinks green to indicate network activity.
Disk Light	Displays a solid green light and blinks during disk activity.
Power Light	Displays a solid green light when the system is powered on.
Reset Button	Push for 5 seconds to reset the Barracuda Backup Server.
Power Button	Push to power on the Barracuda Backup Server, tap to safely reset the Barracuda Backup Server.

The following figure illustrates the Barracuda Backup rear panel ports and connectors for model 490.

Model 490 Rear Panel


USB Ports
USB Ports
Power Supply
Keyboard Port
Dual Link
DVI-D Port
VGA Port
Network Port
Mouse Port

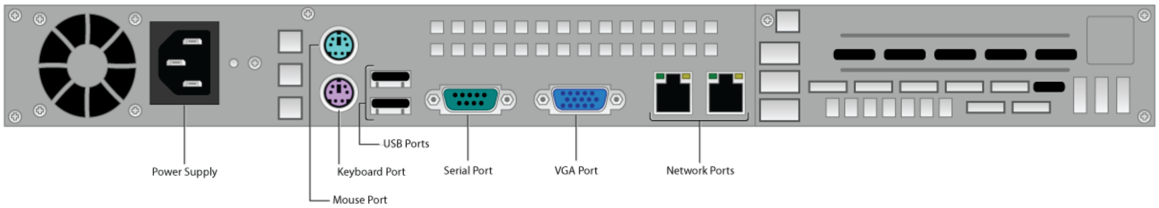
The following table describes the Barracuda Backup rear panel ports and connectors for model 490.

Model 490 Rear Panel Port and Connector Description

Port/Connector Name	Details
Power Supply	Power supply input.
Mouse Port	*Optional*. Mouse port.
Keyboard Port	*Optional*. PS2 keyboard connection.
USB Ports (4)	*Optional.* USB device connection.
Dual Link DVI-D Port	*Optional*. Digital monitor connection.
VGA Port	*Recommended*. Video graphics array (VGA) monitor connection.
Network Port	Network port.

The following figure illustrates the Barracuda Backup rear panel ports and connectors for model 690.

Model 690 Rear Panel


USB Ports
Power Supply
Keyboard Port
Serial Port
VGA Port
Network Ports
Mouse Port

The following table describes the Barracuda Backup rear panel ports and connectors for model 690.

Model 690 Rear Panel Port and Connector Description

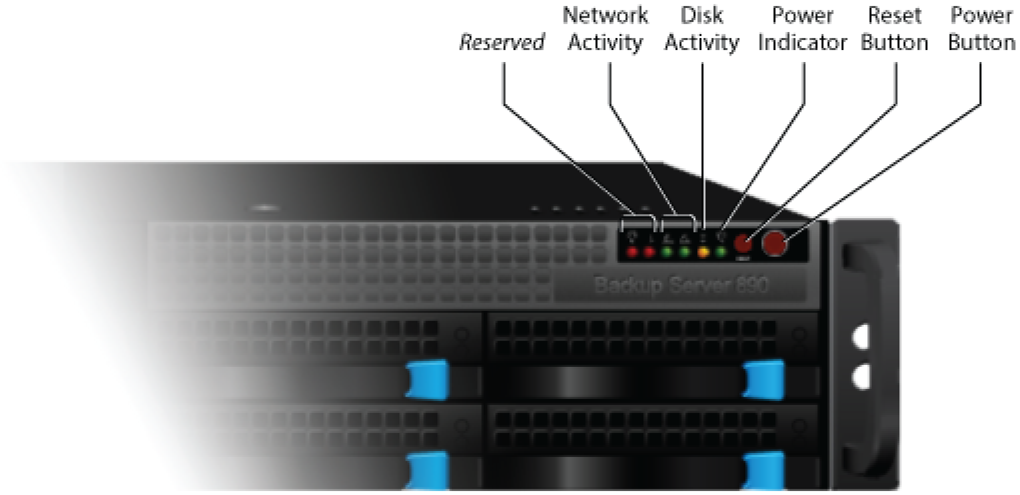
Port/Connector Name	Details
Power Supply	Power supply input.
Mouse Port	*Optional*. Mouse port.
Keyboard Port	*Optional*. PS2 keyboard connection.
USB Ports (2)	*Optional.* USB device connection.

Serial Port	*Optional*. Serial device connection.
VGA Port	*Recommended*. Video graphics array (VGA) monitor connection.
Network Ports (2)	Network ports.

Barracuda Backup Server 890, 891, 892, 990, and 991

The following figure illustrates the Barracuda Backup power and disk activity indicator lights for models 890 through 991.

Model890, 891, 892, 990, and 991 Front Panel



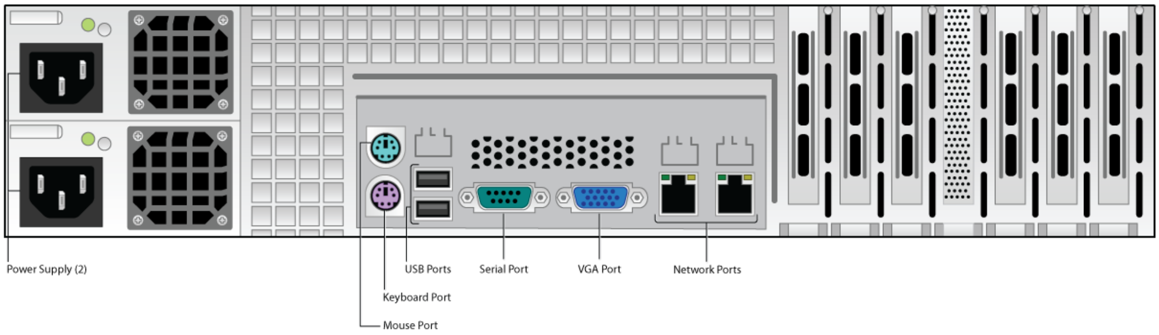
The following table describes the Barracuda Backup front panel indicator lights for models 890, 891, 892, 990, and 991.

Model 890, 891, 892, 990, and 991 Front Panel Component Description

Component Name	Description
Reserved (2)	*Reserved for future use.*
Network Activity (2)	Blinks green to indicate network activity.
Disk Light	Displays a solid green light and blinks during disk activity.
Power Light	Displays a solid green light when the system is powered on.
Reset Button	Push for 5 seconds to reset the Barracuda Backup Server.
Power Button	Push to power on the Barracuda Backup Server, tap to safely reset the Barracuda Backup Server.

The following figure illustrates the Barracuda Backup rear panel ports and connectors for models 890 and 891.

Model 890 and 891 Rear Panel


Power Supply (2)
USB Ports
Serial Port
VGA Port
Network Ports
Keyboard Port
Mouse Port

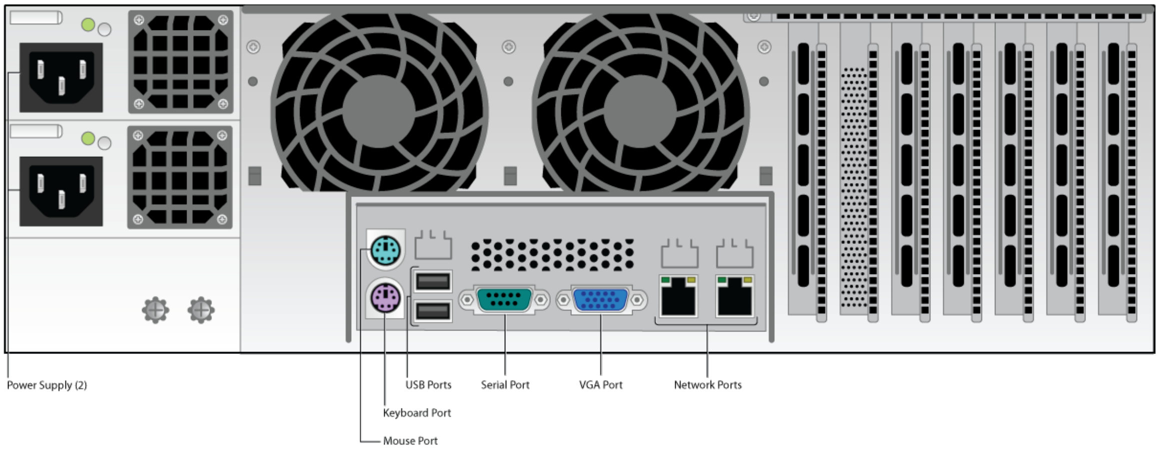
The following table describes the Barracuda Backup rear panel ports and connectors for models 890 and 891.

Model 890 and 891 Rear Panel Port and Connector Description

Port/Connector Name	Description
Power Supply (2)	Redundant power supply input.
Mouse Port	*Optional*. Mouse port.
Keyboard Port	*Optional*. PS2 keyboard connection.
USB Ports (2)	*Optional.* USB device connection.
Serial Port	*Optional*. Serial device connection.
VGA Port	*Recommended*. Video graphics array (VGA) monitor connection.
Network Ports (2)	Network ports.

The following figure illustrates the Barracuda Backup rear panel ports and connectors for models 892, 990 and 991.

Model 892, 990, and 991 Rear Panel


Power Supply (2)
USB Ports
Serial Port
VGA Port
Network Ports
Keyboard Port
Mouse Port

Model 892, 990, and 991 Rear Panel Port and Connector Description

Port/Connector Name	Description
Power Supply (2)	Redundant power supply input.
Mouse Port	*Optional* . Mouse port.
Keyboard Port	*Optional* . PS2 keyboard connection.
USB Ports (2)	*Optional.* USB device connection.

Serial Port	*Optional* . Serial device connection.
VGA Port	*Recommended* . Video graphics array (VGA) monitor connection.
Network Ports (2)	Network ports.

Barracuda Backup Server 1090 and 1091

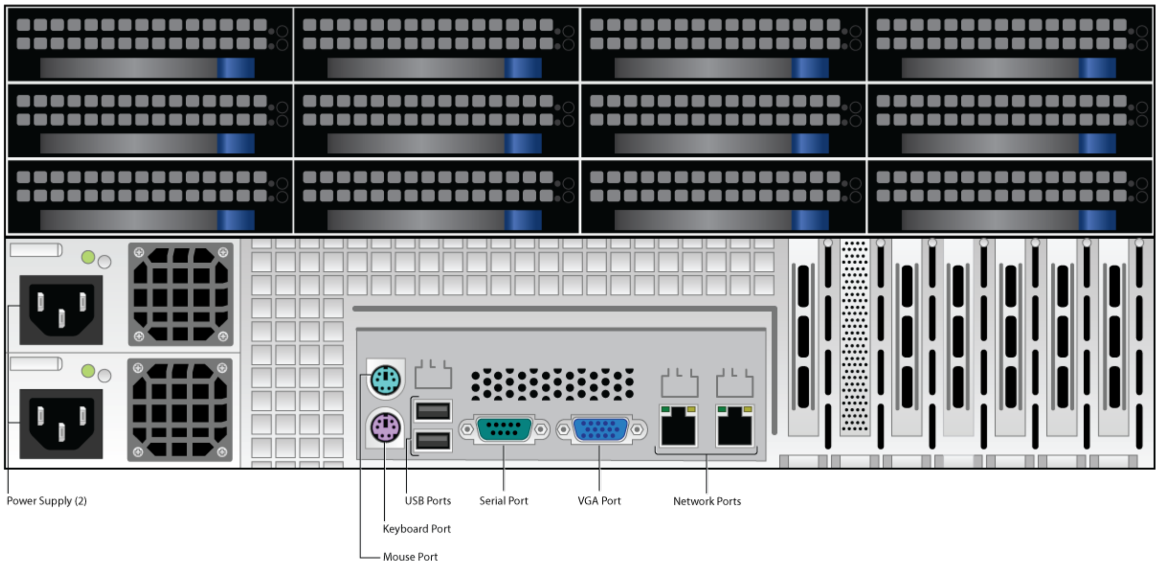
The following table describes the front panel indicator lights for models 1090 and 1091.

Model 1090 and 1091 Front Panel Component Description

Component Name	Description
Reserved (2)	*Reserved for future use.*
Network Activity (2)	Blinks green to indicate network activity.
Disk Light	Displays a solid green light and blinks during disk activity.
Power Light	Displays a solid green light when the system is powered on.
Reset Button	Push for 5 seconds to reset the Barracuda Backup Server.
Power Button	Push to power on the Barracuda Backup Server, tap to safely reset the Barracuda Backup Server.

The following figure illustrates the Barracuda Backup rear panel ports and connectors for models 1090 and 1091.

Model 1090 and 1091 Rear Panel



The following table describes the rear panel ports and connectors for models 1090 and 1091.

Model 1090 and 1091 Rear Panel Port and Connector Description

Port/Connector Name	Description
Power Supply (2)	Redundant power supply input.
Mouse Port	*Optional*. Mouse port.
Keyboard Port	*Optional*. PS2 keyboard connection.
USB Ports (2)	*Optional.* USB device connection.

Serial Port	*Optional*. Serial device connection.
VGA Port	*Recommended*. Video graphics array (VGA) monitor connection.
Network Ports (2)	Network ports.

Barracuda Backup Server Hardware Specifications

This article refers to Barracuda Backup firmware version 5.0 and higher.

In this article:

- Barracuda Backup Form Factor
- Barracuda Backup Server Weight and Dimensions
- Barracuda Backup Server Network Interface Card
- 10 Gigabit Ethernet Card Option (Models 892, 990, and 1090 Only)
- 10 Gigabit Fiber Card Option (Models 891, 991, and 1091 Only)
- Barracuda Backup Server Model 890, 990, and 1090 Drive Layout

Related Articles

- Barracuda Backup Server Panel Indicators, Ports, and Connectors
- How to Physically Install the Barracuda Backup Server

Barracuda Backup Form Factor

Model	Form Factor
190	Rack mountable - 1U
390	Rack mountable - 1U
490	Rack mountable - 1U
690	Rack mountable - 1U
890/891	Rack mountable - 2U
892/990/991	Rack mountable - 3U
1090/1091	Rack mountable - 4U

Barracuda Backup Server Weight and Dimensions

Model	Weight in Pounds	Dimensions in Inches (W x D x H)
190	5.2	10 x 8.3 x 2
390	12	16.8 x 14 x 1.7
490	26	17.2 x 19.8 x 1.7
690	26	17.2 x 19.8 x 1.7
890/891/892	52	17.4 x 25.5 x 3.5
990/991	76	17.2 x 25.5 x 5.2
1090/1091	154	17.2 x 27.4 x 7

Barracuda Backup Server Network Interface Card

Use network interface card (NIC) bonding to increase available bandwidth:

Model	Throughput	Number of Interfaces
190	1Gb	1
390	1Gb	1
490	1Gb	1
690	1Gb	2
890	1Gb	2
891/892	10Gb	3
990/991	10Gb	3
1090/1091	10Gb	3

10 Gigabit Ethernet Card Option (Models 892, 990, and 1090 Only)

Models 892, 990, and 1090 include a 10 Gigabit Ethernet card. If your organization's environment does not support 10 Gigabit throughput, the card reduces its speed to 1 Gigabit:

- **1 Gigabit Connection** - Plug in a CAT5e cable for 1 Gigabit throughput.
- **10 Gigabit Connection** - Plug in a CAT6e cable and a 10 Gigabit switch for 10 Gigabit throughput.

10 Gigabit Fiber Card Option (Models 891, 991, and 1091 Only)

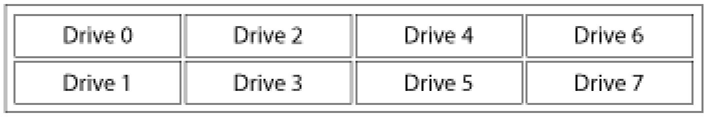
Use a small form-factor pluggable (SFP) transceiver module:

- **SFP** - Use SFP for 1/4 Gigabit/second throughput; you will need a multi-mode cable with LC connections or a direct attach cable.
- **SFP+** - Use SFP+ for 10 gigabit/second throughput (included); you will need a multi-mode cable with LC connections or a direct attach cable.
- **Vendor-Specific SFP** - If you are using a vendor-specific module in your environment, simply remove the Barracuda provided SFP and replace with other vendor.

By default the top port is active. Contact Barracuda Networks Technical Support if you wish to bond the two ports for 20 Gigabit throughput with failover capabilities.

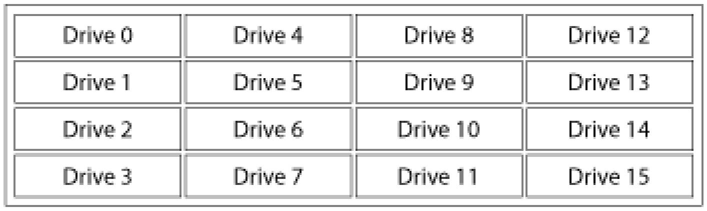
Barracuda Backup Server Model 890, 990, and 1090 Drive Layout

Model 890 Drive Layout



Drive 0	Drive 2	Drive 4	Drive 6
Drive 1	Drive 3	Drive 5	Drive 7

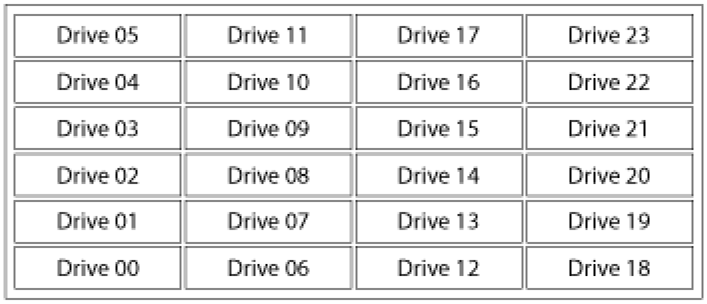
Model 990 Drive Layout



Drive 0	Drive 4	Drive 8	Drive 12
Drive 1	Drive 5	Drive 9	Drive 13
Drive 2	Drive 6	Drive 10	Drive 14
Drive 3	Drive 7	Drive 11	Drive 15

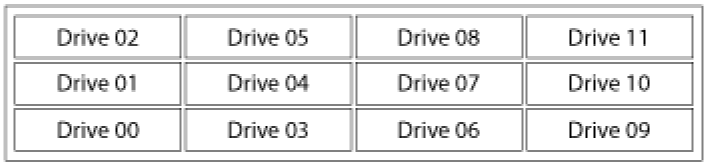
Model 1090 Drive Layout

Device Front – Connector 1



Drive 05	Drive 11	Drive 17	Drive 23
Drive 04	Drive 10	Drive 16	Drive 22
Drive 03	Drive 09	Drive 15	Drive 21
Drive 02	Drive 08	Drive 14	Drive 20
Drive 01	Drive 07	Drive 13	Drive 19
Drive 00	Drive 06	Drive 12	Drive 18

Device Back – Connector 0



Drive 02	Drive 05	Drive 08	Drive 11
Drive 01	Drive 04	Drive 07	Drive 10
Drive 00	Drive 03	Drive 06	Drive 09

AC Input Voltage Range

Model	Power	AC Input Range	BTU/hr
190	Single 60W	12V	205
390	Single 220W	100V	751
490	Single 350W	100-240V	1194
690	Single 350W	100-240V	1194
890/891/892	720W Redundant Power	100-240V	2457
990/991	800W Redundant Power	100-240V	2730
1090/1091	1400W Redundant Power	100-140V 180-240V 120-230V	4777

How to Physically Install the Barracuda Backup Server

This article refers to Barracuda Backup firmware version 5.0 and higher.

In this article:

- Rack Mount Barracuda Backup Server Models 390 through 1091
- Set Up the Barracuda Backup Server

Related Articles

- Barracuda Backup Server Panel Indicators, Ports, and Connectors
- Barracuda Backup Server Hardware Specifications

Rack Mount Barracuda Backup Server Models 390 through 1091

For Barracuda Appliances 390 and above, these rack mounting Instructions provide information on installing the SC825 chassis into a rack unit with the rail kit provided. Refer to the installation instructions that comes with the rack unit for detailed instructions.

Model 190
The Model 190 is a desktop unit and does not require rack mounting.

Choose a Setup Location

- Allow enough clearance in front of the rack to allow the front door to open completely (~25 inches).
- Leave approximately 30 inches of clearance in the back of the rack to allow for sufficient airflow and ease in servicing.
- This product is for installation only in a "Restricted Access Location" (dedicated equipment rooms, service closets and other secure, ventilated environments).
- You must have access to a grounded power outlet.

Rack Mounting Precautions

- Ensure the leveling jacks on the bottom of the rack are fully extended to the floor with the full weight of the rack resting on them.
- In a single rack installation, stabilizers should be attached to the rack.
- In multiple rack installations, the racks should be coupled together.
- Verify the rack is stable before extending a component from the rack.
- Extend only one component at a time - extending two or more simultaneously may cause the rack to become unstable.

General Server Precautions
Review the electrical and general safety precautions that came with the components you are adding to the chassis. Determine the placement of each component in the rack before you install the rails. Install the heaviest server components on the bottom of the rack first, and then work upwards.

Use a regulating uninterruptible power supply (UPS) to protect the server from power surges, voltage spikes, and to keep your system operating in case of a power failure. Allow the hot plug hard drives and power supply modules to cool before touching them. Always keep the rack's front door and all panels and components on the servers closed when not servicing to maintain proper cooling.

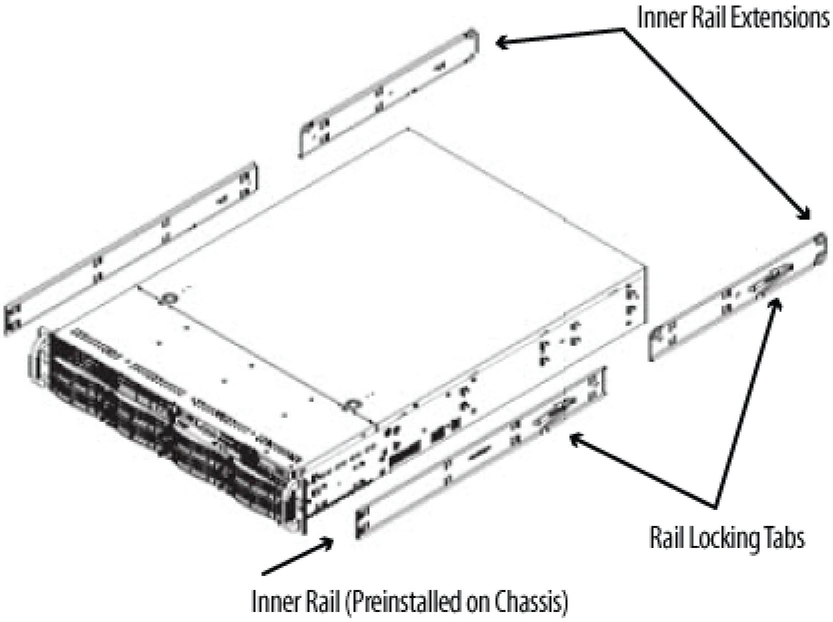
- **Ambient Operating Temperature -** If installed in a closed or multi-unit rack assembly, the ambient operating temperature of the rack environment may be greater than the ambient temperature of the room. Therefore, consideration should be given to installing the equipment in an environment compatible with the manufacturer's maximum rated ambient temperature (Tmra).
- **Proper Airflow and Mechanical Loading** - Mount equipment into a rack so that the amount of airflow required for safe operation is not compromised and to prevent any hazardous condition that can arise due to uneven mechanical loading.
- **Circuit Overloading -** Consideration should be given to the connection of the equipment to the power supply circuitry and the effect that any possible overloading of circuits might have on overcurrent protection and power supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing these concerns.
- **Reliable Ground -** To ensure a reliable ground at all times, the rack itself should be grounded. Particular attention should be given to power supply connections other than the direct connections to the branch circuit (i.e. the use of power strips, etc.).

Install the Barracuda Backup Server into the Rack

This section provides information on installing the SC825 chassis into a rack unit with the provided rails. Refer to the installation instructions that came with the rack unit you are using for detailed instructions; these rails fit a rack between 26" and 33.5" deep.

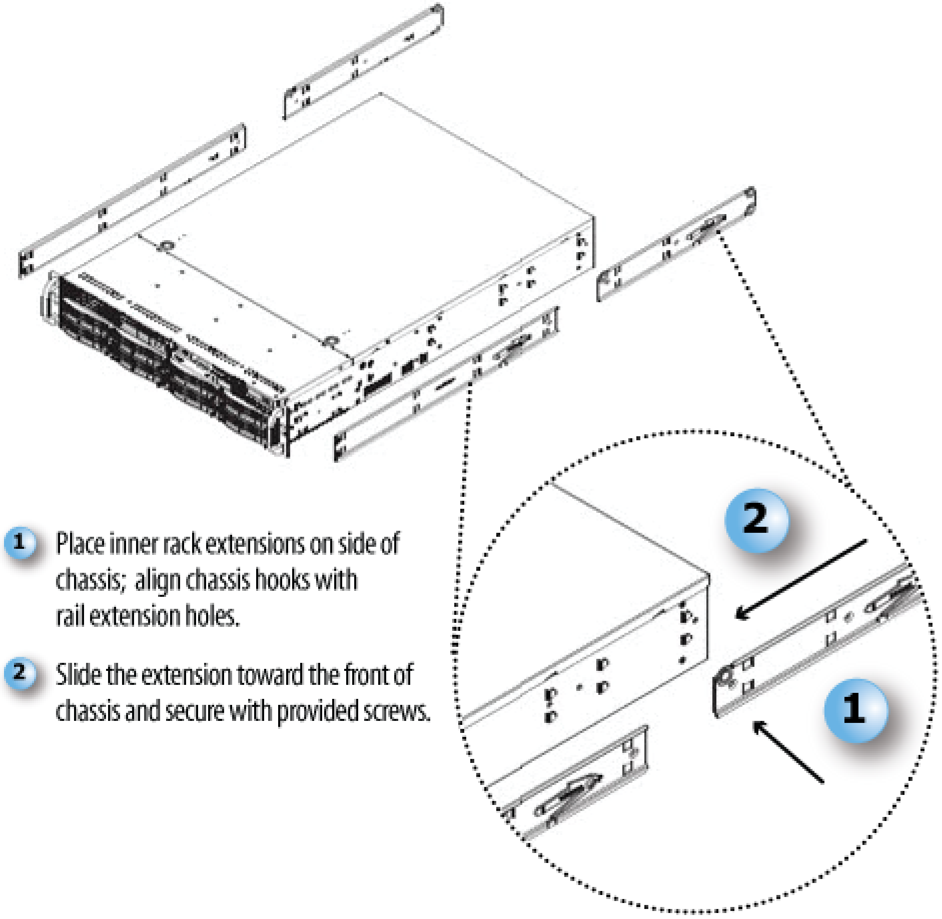
- **Identify the Rack Rail Sections** - The chassis package includes two rack rail assemblies in the rack mounting kit. Each assembly consists of two sections: an inner fixed chassis rail that secures directly to the server chassis, and an outer fixed rack rail that secures directly to the rack itself.

  Rack Rail Sections


Inner Rail Extensions
Rail Locking Tabs
Inner Rail (Preinstalled on Chassis)

- **Locking Tabs** - Both chassis rails have a locking tab. The tabs lock the server into place when it is installed and pushed fully into the rack. These tabs also lock the server into place when fully extended from the rack so as to prevent the server from coming completely out of the rack when pulled out for servicing.

Identifying Rack Rail Sections (right side rail shown)



① Place inner rack extensions on side of chassis; align chassis hooks with rail extension holes.

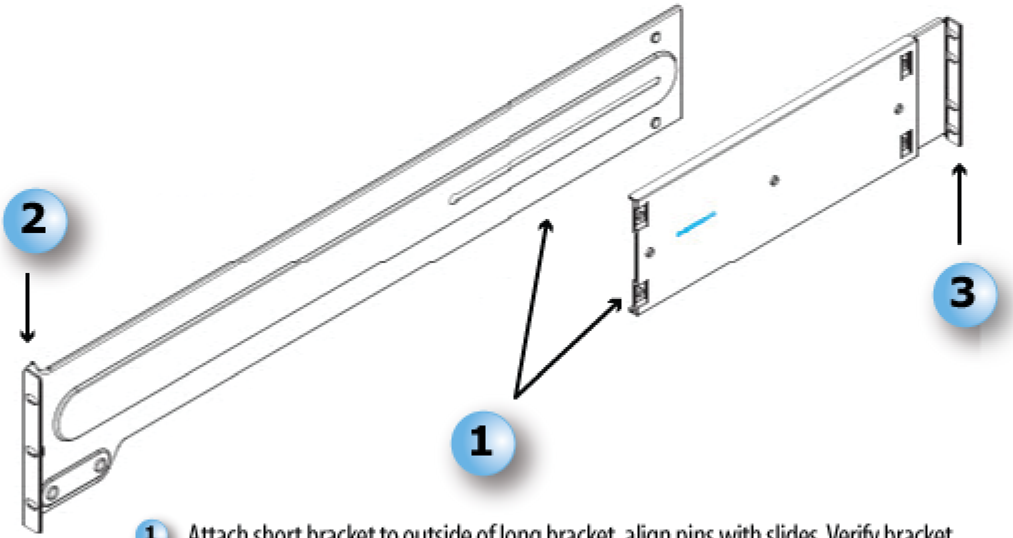
② Slide the extension toward the front of chassis and secure with provided screws.

Install Inner Rail Extension

The SC825 chassis includes a set of inner rails in two sections: inner rails and inner rail extensions.

- **Inner Rack Rails** - The inner rails are pre-attached and do not interfere with normal use of the chassis if you decide not to use a server rack. Attach the inner rail extension to stabilize the chassis within the rack.
  - Place the inner rack extensions on the side of the chassis, aligning the hooks of the chassis with the rail extension holes. Verify the extension faces "outward" like the pre-attached inner rail.
  - Slide the extension toward the front of the chassis, and s ecure the chassis with 2 screws as shown below.
- **Outer Rack Rails** - Outer rails attach to the server rack and hold the server in place. The outer rails for the SC836 chassis extend between 30 inches and 33 inches.
  - Assemble the outer rack rails using the diagram shown below:

Assemble Outer Rack Rails



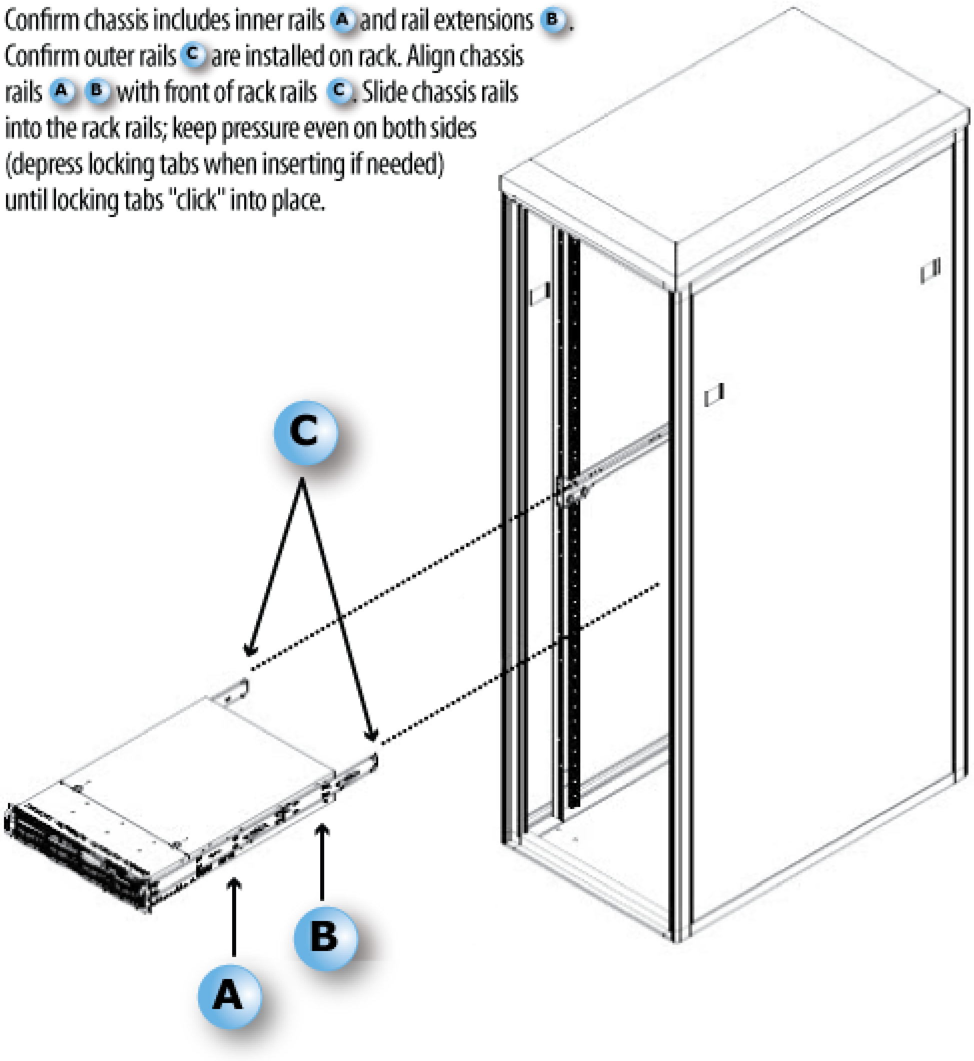
① Attach short bracket to outside of long bracket, align pins with slides. Verify bracket ends face same direction.

② Adjust short and long bracket to proper distance so rail fits snogly into rack, and secure long bracket to front side of outer rail with two M5 screws.

③ Attach short bracket to rear side of outer rail with three M5 screws.

  - Attach the outer rack rails and install the chassis into the rack as illustrated in the following diagram:

Install Chassis into the Rack


Confirm chassis includes inner rails A and rail extensions B.
Confirm outer rails C are installed on rack. Align chassis rails A B with front of rack rails C. Slide chassis rails into the rack rails; keep pressure even on both sides (depress locking tabs when inserting if needed) until locking tabs "click" into place.
C
B
A

Set Up the Barracuda Backup Server

Physically install the Barracuda Backup Server using the following steps:

1. For models 390-1091, fasten the Barracuda Backup Server to a 19-inch rack. For model 190, place it in a stable location.
2. Connect an Ethernet cable from the network switch to the Ethernet port on the back of the Barracuda Backup Server.
3. Connect a standard VGA monitor, PS2/USB keyboard, and an AC power cord to the Barracuda Backup Server.
4. Press the **Power** button to turn the unit on.

For detailed configuration steps, refer to Step 2 in the Getting Started section of this TechLibrary, or the Barracuda Backup Deployment Template.

Troubleshooting and Error Messages

In this Section

- Understanding Why the Barracuda Backup Agent Moves to a New Volume

- Understanding Why Data is not Replicating to an Offsite Barracuda Backup Location
- How to Troubleshoot Using the Barracuda Backup Agent (Windows) Log File
- How to Resolve Low Disk Space
- How to Change the Barracuda Backup Agent Port Number
- How to Change the Barracuda Linux Backup Agent Port Number
- How to Change the SQL Recovery Model
- How to Resolve Microsoft Exchange 2010 Large Message Restore Errors
- How to Resolve Snapshot Backup Errors
- Resolving "Agent database moved to different location" Warning
- Resolving "Error Creating Snapshot" Error During ESX/ESXi Virtual Machine Backup
- Resolving "Error Reading Object" Error During ESX or ESXi Virtual Machine Backup
- Resolving "Error Removing Snapshot" Error During ESX/ESXi Virtual Machine Backup
- Resolving "Failed to connect to backup agent software" Error
- Resolving "File System Snapshot was Released" Error
- Resolving "Incremental backups cannot be performed while circular logging is enabled" Error
- Resolving “An error occurred during agent backup initialization" Error
- Resolving "Unable to back up virtual machines with independent disks" Error
- Resolving "VMDK is larger than the maximum size supported by datastore" Error
- Resolving "Error backing up selected object" Error
- Resolving "An unknown OS error occurred" Error
- Resolve the "Failure while using USN journal" Error
- Monitoring Windows System Performance During Backup
- How to Increase Backup Performance

Related Articles

- Replacing a Failed Barracuda Backup Server
- VMware Data Recovery Backup and Restore Permissions

Understanding Why the Barracuda Backup Agent Moves to a New Volume

The Barracuda Backup Agent requires at least 1GB of free disk space on a data source for its database. If less than the required amount of disk space is available, the Barracuda Agent database is automatically moved to another storage volume.

While backups will continue to run, a warning message displays in the Barracuda Backup web interface stating that the database has been moved:

Warnings
⚠ 1 Warning

Agent - *Agent database moved to different location*

To resolve this issue, install the Barracuda Backup Agent to an alternate storage volume with adequate free disk space.

Updating the Backup Agent Location

Use the following steps to move the Barracuda Backup Agent to an alternate storage volume and eliminate the warning message:

1. Completely uninstall the Barracuda Backup Agent using the **Add/Remove Programs** or **Programs and Features** option on your system.
2. Once the Agent is uninstalled, log in to the Barracuda Backup web interface, and go to the **SUPPORT > Software Downloads** page.
3. Download and install the latest version of the Barracuda Backup Agent.
4. During installation, select the installation path on a storage volume with at least 1GB of free disk space.
5. Once the next successful backup occurs, the warning message no longer displays.

Understanding Why Data is not Replicating to an Offsite Barracuda Backup Location

This article refers to firmware version 5.0 and higher.

The Barracuda Backup default rate limit controls the rate of data replicated to offsite storage locations throughout the day; preserving Internet bandwidth during peak usage and optimizing offsite backup transfers during daily non-peak hours. You can further refine the rate limit by enabling an alternate rate limit and specifying a specific time period to which it applies.

However, if a large backup is scheduled during the alternate rate limit time interval, replication to the offsite location may not complete within the specified time period. In this case, the yellow status indicator (⚠) icon displays on the **STATUS** page indicating there is a problem with the offsite syncing queue.

Resolving Data Replication Issue

To resolve this issue, you can:

- Increase Speed Limit
- Reduce Amount of Data for Replication
- Decrease Backup Schedule Frequency

Increase Speed Limit

Use the following steps to increase the speed limit to ensure data replication finishes within the specified timeframe:

1. Log in to Barracuda Backup, and go to **BACKUP > Rate Limit** page.
2. Turn on **Alternate Rate Limit**, and update the bandwidth based on the selected option:
    - **Full Speed** - Uses 100% of available bandwidth
    - **Smart Mode** - Increase the **Percent of Bandwidth** value
    - **Kb/s or Mb/s** - Specify a higher value
3. Click **Save** at the top of the page to save your changes.

Reduce Amount of Data for Replication

Use the following steps to select less data for replication:

1. Log in to Barracuda Backup, and go to **BACKUP > Sources**.
2. On the **Data Sources** page, locate the data source on the system you wish to modify, and click **Edit** to the right of the data source.
3. In the **Edit** page, in the **Item Selection** section, review the selected items. Determine if there are items that do not need backup, and deselect those items.
4. Click **Save** at the top of the page to save your changes.

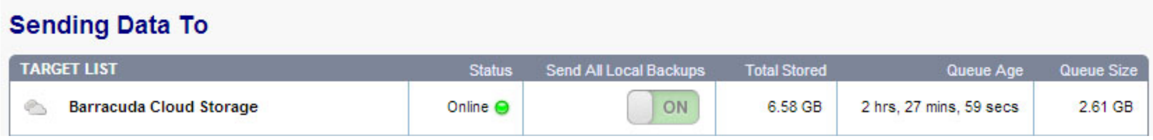
Decrease Backup Schedule Frequency

1. Log in to Barracuda Backup, and go to **BACKUP > Schedule**.
2. Click the **Edit** (✎) icon to the right of the schedule associated with the backup.
3. In the **Edit Backup Schedule** page, if **Repeat** is turned on in the **Daily Backup Timeline** section, reduce the minute or hour frequency.
4. Click **Save** at the top of the page to save your changes.

How to View Offsite Transfer Statistics

To view transfer statistics, log in to Barracuda Backup, and go to **BACKUP > Replication**. The following queue details display:

- **Status** - Displays either the green indicator (Online ●) icon or the red indicator (Offline ■) icon
- **Total Stored** - Total size of file parts transferred offsite from the Barracuda Backup Server
- **Queue Age** - Amount of time that the queued data has been waiting to be transferred offsite from the Barracuda Backup Server
- **Queue Size** - Total size of the file parts yet to be transferred offsite from the Barracuda Backup Server



Sending Data To

TARGET LIST	Status	Send All Local Backups	Total Stored	Queue Age	Queue Size
Barracuda Cloud Storage	Online ●	ON	6.58 GB	2 hrs, 27 mins, 59 secs	2.61 GB

How to Troubleshoot Using the Barracuda Backup Agent (Windows) Log File

This article refers to Barracuda Backup firmware version 5.2 and higher, and the Barracuda Backup Agent (Windows) version 5.2 and higher.

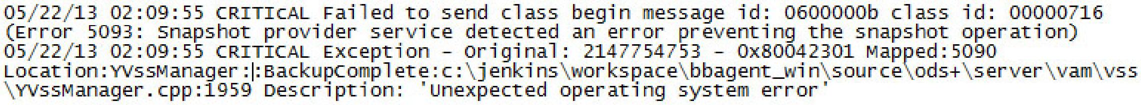
Use the Backup Agent **bbtrace.txt** log files to understand and resolve any errors that may occur with the Backup Agent such as an Agent backup initialization error. Each time the Backup Agent Service is restarted, a number is appended to the current **bbtrace.txt** file, and a new file is generated.

To review the log file:

1. Log in to the data source that is failing to back up data, and go to the Backup Agent log files. By default, the log files are located in: **C:\Program Files\Barracuda\Barracuda Backup Agent\log**
2. Locate the file **bbtrace.txt**; this is the most recent log file.

   If the server was rebooted, or the agent was restarted, you may need to review older **bbtrace.txt** files to find the time listed in the **Report** details page in the previous step.

3. Open **bbtrace.txt** in Notepad. This file contains data that is helpful in determining the specific error. Each log entry is time stamped, so you will first want to identify when the failed backup occurred based on the **Report** details page; note that there may be multiple days of log details so it is recommended that you use the search function to find the error.
4. Search the log file for terms such as **Failed** or **Critical**. Once you locate the term, review the associated content to determine the specific error message:

   ```
   05/22/13 02:09:55 CRITICAL Failed to send class begin message id: 0600000b class id: 00000716
   (Error 5093: Snapshot provider service detected an error preventing the snapshot operation)
   05/22/13 02:09:55 CRITICAL Exception - Original: 2147754753 - 0x80042301 Mapped:5090
   Location:YVssManager::BackupComplete:c:\jenkins\workspace\bbagent_win\source\ods+\server\vam\vss
   \YVssManager.cpp:1959 Description: 'Unexpected operating system error'
   ```

   In this example, a VSS snapshot failed due to an unexpected operating system error on the targeted server.

   Note that an Agent error message is typically followed by associated `CRITICAL Sup: Resource not put` details which is not needed for troubleshooting.

How to Resolve Low Disk Space

This article applies to all firmware versions, except where noted.

If the Barracuda Backup Server drives run out of space, backups cannot complete and will fail. A low disk space notification is sent when the Barracuda Backup server reaches 80% capacity and above. Following are several options to combat this issue:

- Verify a retention policy is applied to all data sources. If a source does not have a retention policy applied to it, all data from that source is retained forever.
  - For example, if you initially back up 100GB of data and 5GB of changed data daily, after 30 days with no retention policy you will have a total of 250GB for the source.
  - Go to the **BACKUP > Retention Policies** page in the web interface and verify that each source has a retention policy applied to it.
  - Additionally, you can contact Barracuda Networks Technical Support and request verification that each data source on the Barracuda Backup Server has a policy applied.

- Determine which data sources are backing up the largest files.
  - In firmware version 5.1 and higher, go to **REPORTS > Large Items** to review which sources are backing up the largest files. You can then determine if these files need to be backed up and exclude them, or lower the retention policy applied to the source.
  - For firmware version 5.0 and lower, contact Barracuda Networks Technical Support and request to have a report of large items generated.

- Determine which Servers are using the most space.
  - Contact Barracuda Networks Technical Support and request to have a usage report generated for your Barracuda Backup Server. This report displays the amount of space used by each backup data source. Additionally, this report shows which Server is retaining the most historic data kept per the retention policy.
  - Modify your retention policies by source basis to manage disk usage.

If you determine that all of the above suggestions are in place and all settings are correct, and you are continuing to run low on space, it may be time to look at upgrading to the next model with increased disk capacity.

> ⓘ If you are unable to determine what is causing your server to run low on space, contact Barracuda Networks Technical Support and a technician can assist with troubleshooting.

How to Change the Barracuda Backup Agent Port Number

> This article refers to Barracuda Backup firmware version 5.0 and higher. This article describes how to resolve the service start error 112.

Issue

You encounter the following error when installing the Barracuda Backup Agent on a server or workstation in your environment:

```
Barracuda Backup Agent setup received error "112 Service Error" while attempting to start service.
```

Cause

You may be running software that uses port 5120 on the selected system which is causing a conflict and generating the error.

Solution

If port 5120 is in use by another piece of software on your data source, Barracuda Networks recommends configuring the Barracuda Backup Agent to use port 5121.

Step 1. Determine the Ports Used by the System

Use the following steps to configure the port:

1. Log in to the system where you received the error, and launch a web browser.
2. Go to the downloads page on the Microsoft TechNet site, and download and install TCPView.
3. Launch TCPView; the ports that the system is currently using display in the web interface.
4. Review the list. If you see that port 5120 is in use, change the port number in the **bbconfig.ini** file as described in **step 2**.

Step 2. Add the Alternate Port Number bbconfig.ini

Use the following steps to change the port number through the **bbconfig.ini** file:

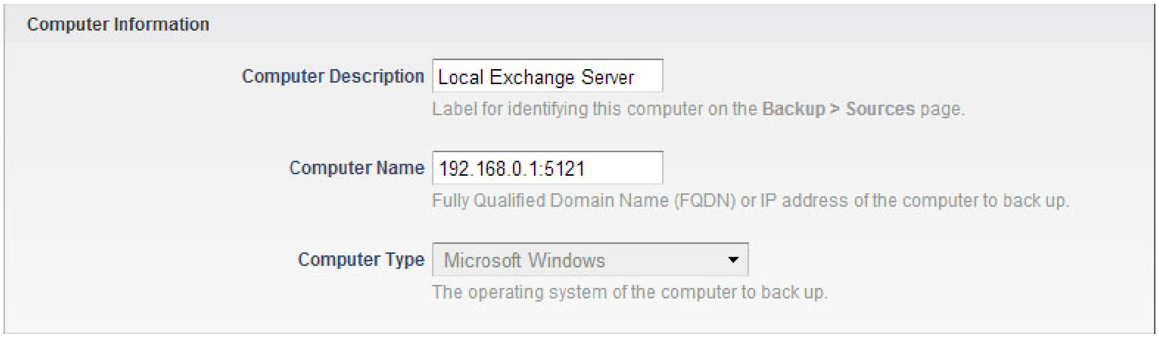
1. On the system where you received the error, locate the **bbconfig.ini** file, usually found in the **C:\Program Files\Barracuda\Barracuda Backup Agent\config** folder.
2. Open **bbconfig.ini** in Notepad, and add the line `port='port number'` beneath the `[configuration]` options. For example:
   ```
   [configuration]
   nodeGuide={XXXXXXXX-XXXXXXXX-XXXXXXXX-XXXXXXXX}
   port=5121
   ```
3. Save and close the file.

Step 3. Restart Services

1. Log in to the system again.
2. Restart the Barracuda Backup Agent service.

Step 4. Update Data source

1. Log in to Barracuda Backup, select the associated Barracuda Backup Server in the left pane, and go to the **BACKUP > Sources** page.
2. In the right pane, click **Edit** to the right of the system where the error occurred.
3. In the **Computer Name** field, append the IP address with the port number added in **Step 2** above.
   For example, if your IP address is '192.168.0.1', and you added the line 'port=5121' to the **bbconfig.ini** file, update the **Computer Name** field as follows:



Computer Information

Computer Description: Local Exchange Server
Label for identifying this computer on the **Backup > Sources** page.

Computer Name: 192.168.0.1:5121
Fully Qualified Domain Name (FQDN) or IP address of the computer to back up.

Computer Type: Microsoft Windows
The operating system of the computer to back up.

How to Change the Barracuda Linux Backup Agent Port Number

> This article refers to Barracuda Backup firmware version 5.3 and higher, and the Barracuda Backup Agent (Linux).

By default the Barracuda Backup Agent (Linux) utilizes port 5120 to communicate with the Barracuda Backup Server. If there is a port conflict with another service, assign the Linux Agent a different port.

Assign a New Port

1. Locate the **bbconfig.ini** file in the default file location: **/usr/local/barracuda/bbs/config/bbconfig.ini**
2. To view the file, type the following command: `cat /usr/local/barracuda/bbs/config/bbconfig.ini`
3. The file content displays:
   ```
   [installControl]
   buildNumber=85471
   installedVersion=5.3.01-rel

   [configuration]
   nodeGuid={00001001-5476F68E-5476F68E-5476F68F}
   ```
4. Open the file with a text editor such as vi or vim, for example: `vim /usr/local/barracuda/bbs/config/bbconfig.ini`
5. Add the following line to the end of the **bbconfig.ini** file: `Port=5555`
   Where *5555* represents the port number you wish to assign the Agent.
6. View the file, it should look similar to:
   ```
   [installControl]
   buildNumber=85471
   installedVersion=5.3.01-rel

   [configuration]
    Port=5555
   ```
7. Save and close the file.

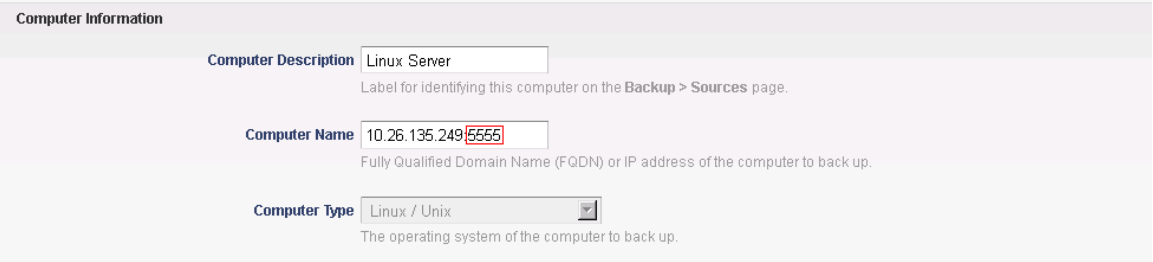
Restart the Agent

Enter the following command to restart the Linux Agent:

```
/etc/init.d/bbagent start
```

Edit the Data Source

1. Log in to the Barracuda Backup web interface, and go to the **BACKUP > Sources** page.
2. Click **Edit** next to the data source, and configure the new port that the Linux Agent is to use, for example:


Computer Information

Computer Description: Linux Server
Label for identifying this computer on the **Backup > Sources** page.

Computer Name: 10.26.135.249:5555
Fully Qualified Domain Name (FQDN) or IP address of the computer to back up.

Computer Type: Linux / Unix
The operating system of the computer to back up.

How to Change the SQL Recovery Model

This article refers to all Barracuda Backup firmware, and Microsoft® SQL Server® 2005, 2008, 2008 R2, or 2012.

In this article:

- Warning Message
- Set the SQL Recovery Model

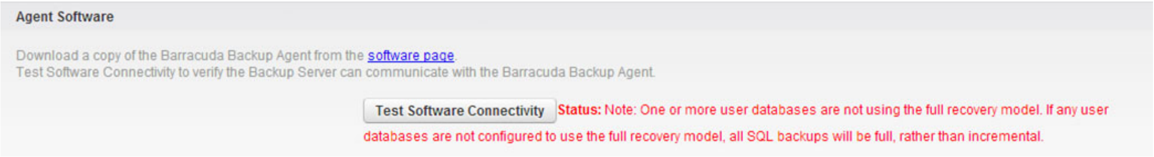
Additional Resource

- SQL Server 2012
- SQL Server 2008 R2
- SQL Server 2008
- SQL Server 2005

The Barracuda Backup Server is designed to initially complete a full backup of the SQL Server database(s). Once the initial full backup is complete, the Barracuda Backup Server can attempt to complete an incremental backup of the SQL Server database. In order for the Barracuda Backup Server to successfully complete an incremental backup, the SQL Server database(s) must be set to *Full Recovery Model*. Typically, SQL Server databases are set to **Simple Recovery Model** by default.

Warning Message

If an incremental backup cannot be completed, the Barracuda Backup Server reverts to a full backup and a warning message displays:


Agent Software

Download a copy of the Barracuda Backup Agent from the software page.
Test Software Connectivity to verify the Backup Server can communicate with the Barracuda Backup Agent.

Status: Note: One or more user databases are not using the full recovery model. If any user databases are not configured to use the full recovery model, all SQL backups will be full, rather than incremental.

Simple Recovery Model
If you wish to leave the SQL Recovery Model set to Simple Recovery Model, log into the Barracuda Backup web interface, and go to the **BACKUP > Schedules** page. On the **Schedules** page, Click the **Edit** icon for the associated backup schedule. On the **Edit** page, in the **SQL/Exchange Backup** section, select **Full** from the **Backup type** drop-down menu. Click **Save** at the top of the page to save your changes.

The recovery model controls how transaction logs are managed. Before changing the Recovery Model, consult your database administrator to determine the setting that is appropriate for your environment.

Set the SQL Recovery Model

All SQL databases need to be set to Full Recovery Model in order to produce Incremental backups. Otherwise, Full backups are performed on every run.

Use the following steps to set the Recovery Model on your SQL databases to Full:

1. Connect to the appropriate instance of the Microsoft SQL Server Database Engine.
2. In Object Explorer, click the server name to expand the server tree.
3. Expand **Databases**, and, depending on the database, either select a user database or expand **System Databases** and select a system database.
4. Right-click the database, and then click **Properties**; the **Database Properties** dialog box displays.
5. In the **Select a Page** pane, click **Options**.
6. The current recovery model displays in the **Recovery Model** list. Select **Full** from the list, and click **OK** to save your changes.

How to Resolve Microsoft Exchange 2010 Large Message Restore Errors

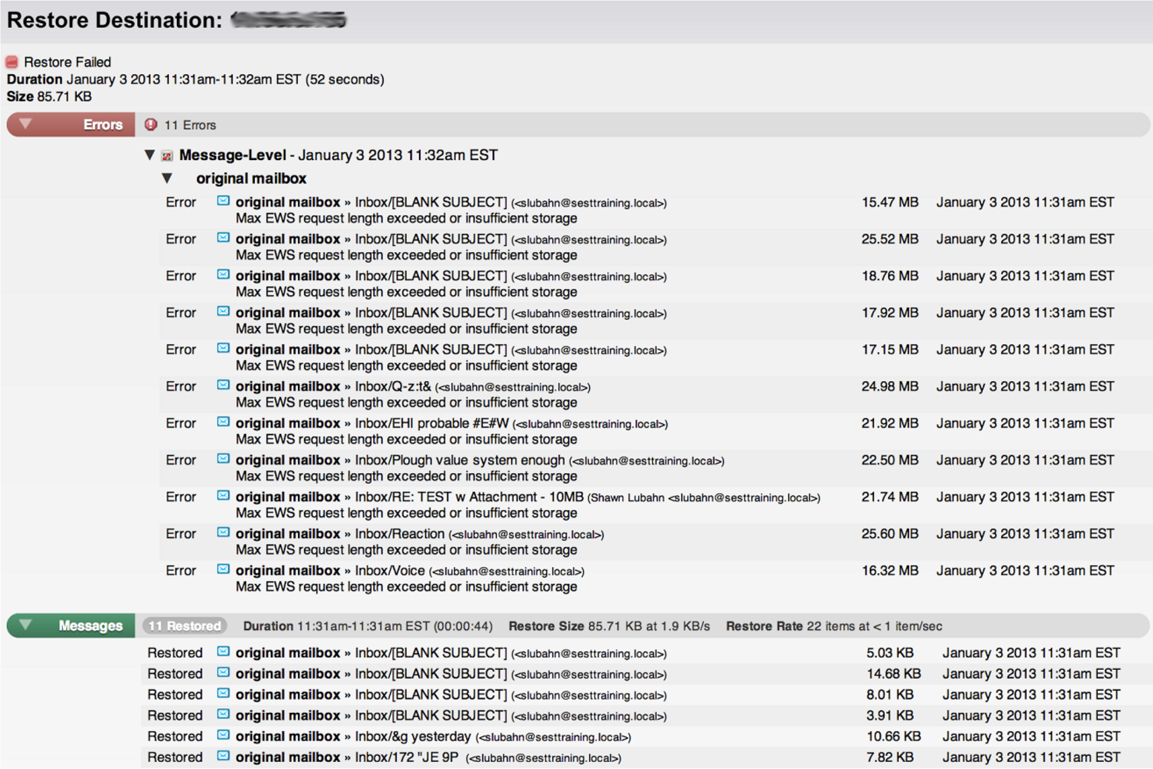
This article refers to firmware 5.0 and higher, and Microsoft® Exchange Server 2010 successfully running message-level backups.

In this article:

- Error Message
- Modify web.config
- Run appcmd
- Barracuda Backup Restore
- Configuration Settings
  - Verify Exchange Management Console Settings
  - Exchange Management Shell

Error Message

If you attempt to restore large messages from Microsoft Exchange 2010, you may encounter a **Max EWS Request** error:



Restore Destination: [redacted]

Restore Failed
Duration January 3 2013 11:31am-11:32am EST (52 seconds)
Size 85.71 KB

11 Errors

Message-Level - January 3 2013 11:32am EST

original mailbox

Error	**original mailbox** » Inbox/[BLANK SUBJECT] (<slubahn@sesttraining.local>) Max EWS request length exceeded or insufficient storage	15.47 MB	January 3 2013 11:31am EST
Error	**original mailbox** » Inbox/[BLANK SUBJECT] (<slubahn@sesttraining.local>) Max EWS request length exceeded or insufficient storage	25.52 MB	January 3 2013 11:31am EST
Error	**original mailbox** » Inbox/[BLANK SUBJECT] (<slubahn@sesttraining.local>) Max EWS request length exceeded or insufficient storage	18.76 MB	January 3 2013 11:31am EST
Error	**original mailbox** » Inbox/[BLANK SUBJECT] (<slubahn@sesttraining.local>) Max EWS request length exceeded or insufficient storage	17.92 MB	January 3 2013 11:31am EST
Error	**original mailbox** » Inbox/[BLANK SUBJECT] (<slubahn@sesttraining.local>) Max EWS request length exceeded or insufficient storage	17.15 MB	January 3 2013 11:31am EST
Error	**original mailbox** » Inbox/Q-z:t& (<slubahn@sesttraining.local>) Max EWS request length exceeded or insufficient storage	24.98 MB	January 3 2013 11:31am EST
Error	**original mailbox** » Inbox/EHI probable #E#W (<slubahn@sesttraining.local>) Max EWS request length exceeded or insufficient storage	21.92 MB	January 3 2013 11:31am EST
Error	**original mailbox** » Inbox/Plough value system enough (<slubahn@sesttraining.local>) Max EWS request length exceeded or insufficient storage	22.50 MB	January 3 2013 11:31am EST
Error	**original mailbox** » Inbox/RE: TEST w Attachment - 10MB (Shawn Lubahn <slubahn@sesttraining.local>) Max EWS request length exceeded or insufficient storage	21.74 MB	January 3 2013 11:31am EST
Error	**original mailbox** » Inbox/Reaction (<slubahn@sesttraining.local>) Max EWS request length exceeded or insufficient storage	25.60 MB	January 3 2013 11:31am EST
Error	**original mailbox** » Inbox/Voice (<slubahn@sesttraining.local>) Max EWS request length exceeded or insufficient storage	16.32 MB	January 3 2013 11:31am EST

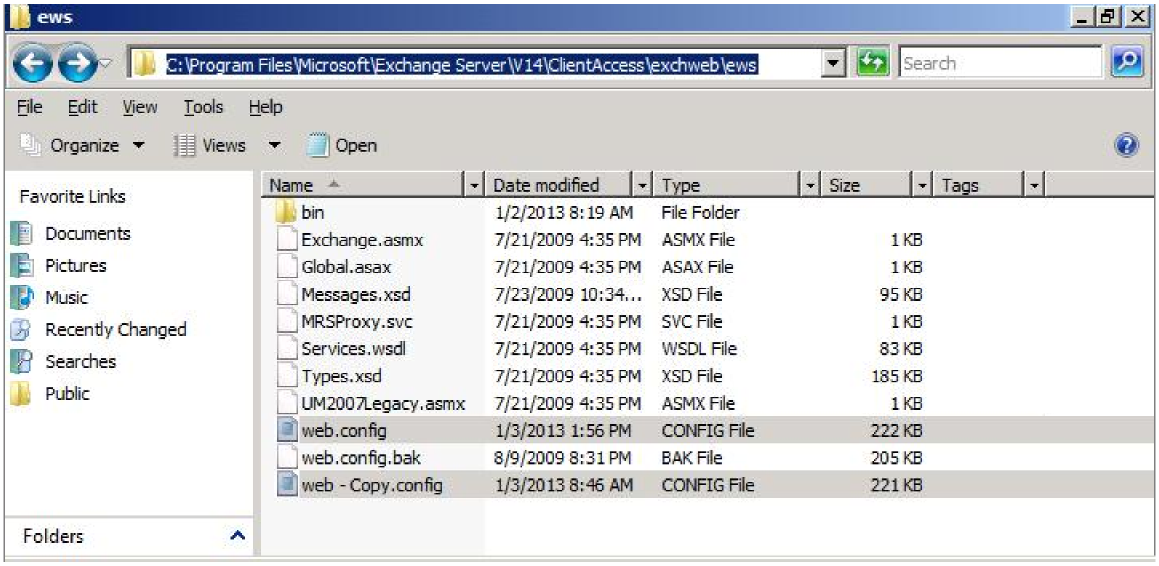
Duration 11:31am-11:31am EST (00:00:44) **Restore Size** 85.71 KB at 1.9 KB/s **Restore Rate** 22 items at < 1 item/sec

Restored	**original mailbox** » Inbox/[BLANK SUBJECT] (<slubahn@sesttraining.local>)	5.03 KB	January 3 2013 11:31am EST
Restored	**original mailbox** » Inbox/[BLANK SUBJECT] (<slubahn@sesttraining.local>)	14.68 KB	January 3 2013 11:31am EST
Restored	**original mailbox** » Inbox/[BLANK SUBJECT] (<slubahn@sesttraining.local>)	8.01 KB	January 3 2013 11:31am EST
Restored	**original mailbox** » Inbox/[BLANK SUBJECT] (<slubahn@sesttraining.local>)	3.91 KB	January 3 2013 11:31am EST
Restored	**original mailbox** » Inbox/&g yesterday (<slubahn@sesttraining.local>)	10.66 KB	January 3 2013 11:31am EST
Restored	**original mailbox** » Inbox/172 "JE 9P (<slubahn@sesttraining.local>)	7.82 KB	January 3 2013 11:31am EST

Modify web.config

Use the following steps to resolve a failed restore:

1. Log into your Microsoft Exchange 2010 Server as the administrator, and navigate to the **Program Files > Microsoft > Exchange Server > V14 > Client Access > exchweb > ews** folder, and create a copy of the file **web.config**:

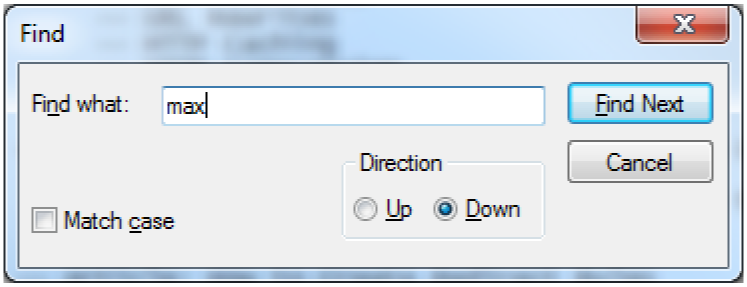

ews
Search
File
Edit
View
Tools
Help
Organize
Views
Open
Favorite Links
Documents
Pictures
Music
Recently Changed
Searches
Public
Folders

C:\Program Files\Microsoft\Exchange Server\V14\ClientAccess\exchweb\ews

Name	Date modified	Type	Size	Tags
bin	1/2/2013 8:19 AM	File Folder		
Exchange.asmx	7/21/2009 4:35 PM	ASMX File	1 KB	
Global.asax	7/21/2009 4:35 PM	ASAX File	1 KB	
Messages.xsd	7/23/2009 10:34...	XSD File	95 KB	
MRSProxy.svc	7/21/2009 4:35 PM	SVC File	1 KB	
Services.wsdl	7/21/2009 4:35 PM	WSDL File	83 KB	
Types.xsd	7/21/2009 4:35 PM	XSD File	185 KB	
UM2007Legacy.asmx	7/21/2009 4:35 PM	ASMX File	1 KB	
web.config	1/3/2013 1:56 PM	CONFIG File	222 KB	
web.config.bak	8/9/2009 8:31 PM	BAK File	205 KB	
web - Copy.config	1/3/2013 8:46 AM	CONFIG File	221 KB	

ⓘ Creating a copy of the **web.config** file allows you to revert to your original settings in case you encounter issues during resolution of the restore error.

2. Open the original **web.config** file using **Notepad** running as the administrator.
3. In **Notepad**, go to **Edit > Find**, and enter `max` in the **find what** field:

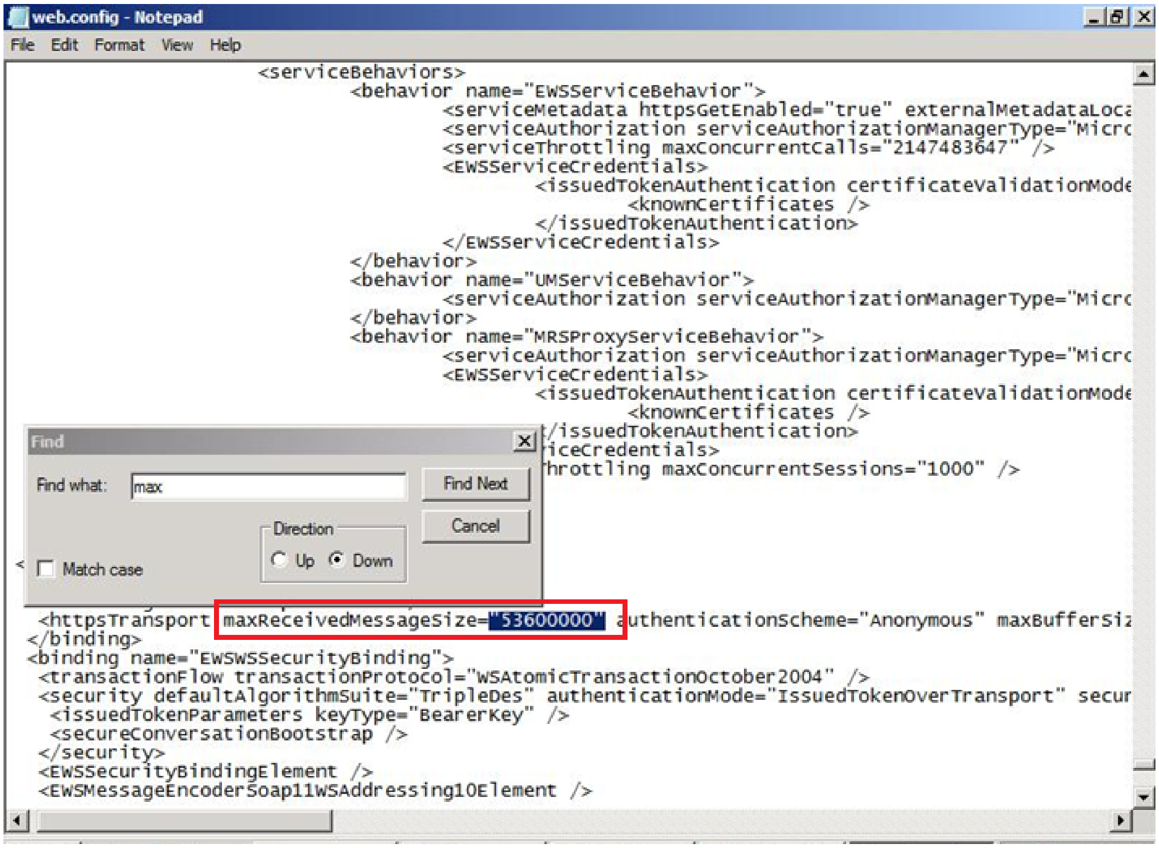

Find
Find Next
Cancel
Direction

Find what: max

☐ Match case

Direction: ○ Up ● Down

4. Click **Find Next** until you locate the following line of code:
`<httpsTransport maxReceivedMessageSize="13600000" authenticationScheme="Anonymous" maxBufferSize="81920" transferMode="Streamed" />`
5. The value `maxReceivedMessageSize="13600000"` represents a maximum attachment size of 13MB. Therefore, any attachments over 13MB cannot be restored. Change this value to a larger value to handle the largest attachment failing to restore, for example, replace `13600000` with `53600000` which allows for attachments just over 50MB:



Find what: max

○ Up ● Down

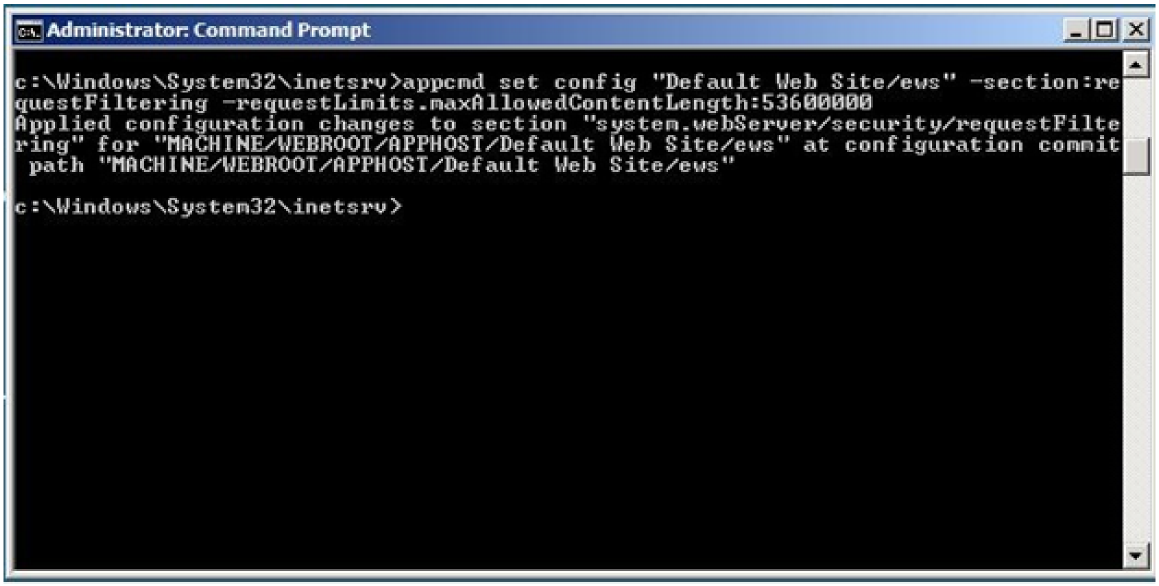
☐ Match case

```
                        <serviceBehaviors>
                                <behavior name="EWSServiceBehavior">
                                        <serviceMetadata httpsGetEnabled="true" externalMetadataLoca
                                        <serviceAuthorization serviceAuthorizationManagerType="Micro
                                        <serviceThrottling maxConcurrentCalls="2147483647" />
                                        <EWSServiceCredentials>
                                                <issuedTokenAuthentication certificateValidationMode
                                                        <knownCertificates />
                                                </issuedTokenAuthentication>
                                        </EWSServiceCredentials>
                                </behavior>
                                <behavior name="UMServiceBehavior">
                                        <serviceAuthorization serviceAuthorizationManagerType="Micro
                                </behavior>
                                <behavior name="MRSProxyServiceBehavior">
                                        <serviceAuthorization serviceAuthorizationManagerType="Micro
                                        <EWSServiceCredentials>
                                                <issuedTokenAuthentication certificateValidationMode
                                                        <knownCertificates />
                                                t/issuedTokenAuthentication>
                                        iceCredentials>
                                        hrottling maxConcurrentSessions="1000" />
 <
  <httpsTransport maxReceivedMessageSize="53600000" authenticationScheme="Anonymous" maxBufferSiz
 </binding>
 <binding name="EWSWSSecurityBinding">
  <transactionFlow transactionProtocol="WSAtomicTransactionOctober2004" />
  <security defaultAlgorithmSuite="TripleDes" authenticationMode="IssuedTokenOverTransport" secur
   <issuedTokenParameters keyType="BearerKey" />
   <secureConversationBootstrap />
  </security>
  <EWSSecurityBindingElement />
  <EWSMessageEncoderSoap11WSAddressing10Element />
```

6. Click **Find Next** until you locate the following line of code:
   `<httpsTransport maxReceivedMessageSize="13600000" authenticationScheme="Anonymous" maxBufferSize="81920" transferMode="Streamed" />`
7. Replace `13600000` with the same value you entered in step 5 above, for example, `53600000` .
8. Click **Find Next** once again until you locate the following line of code:
   `<requestLimits maxAllowedContentLength="13600000" />`
9. Replace `13600000` with the same value you entered in step 5 above, for example, `53600000` .
   Click **File > Save**, and close Notepad.

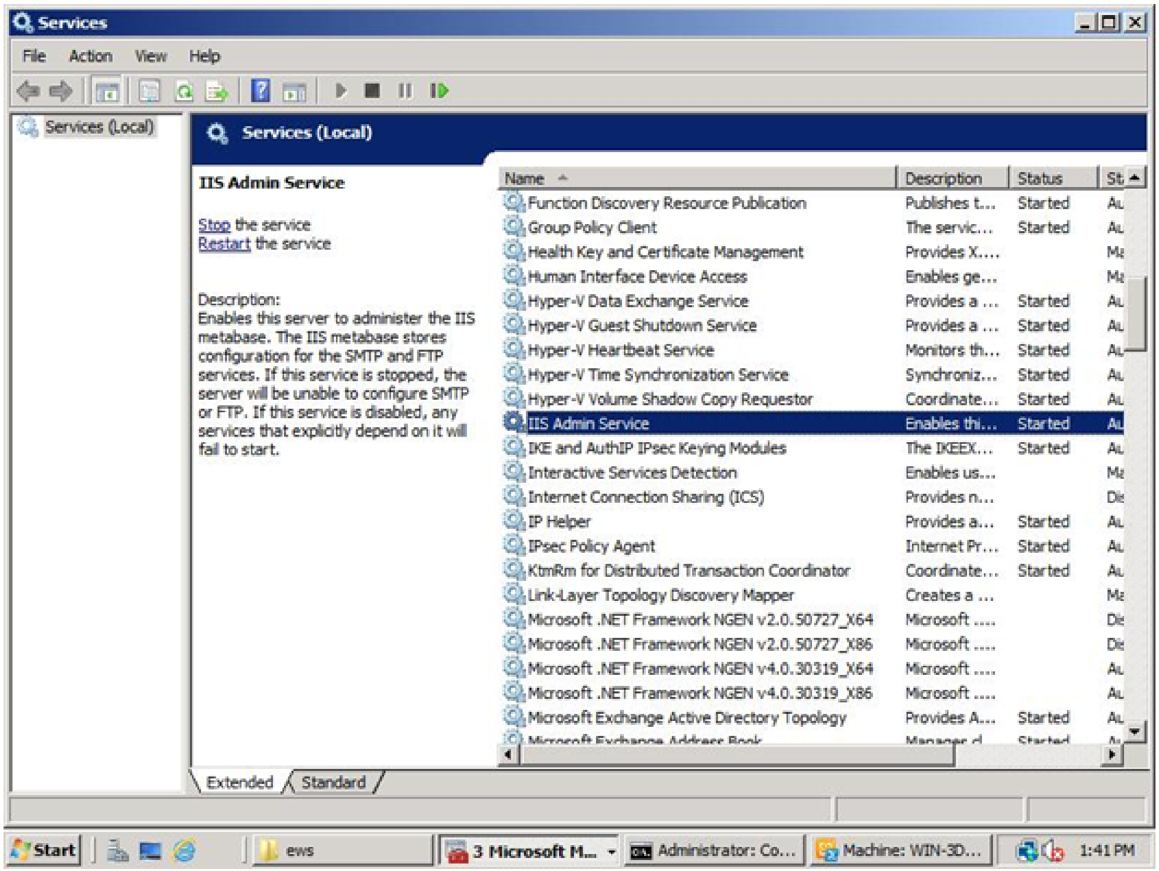
Run appcmd

1. Log into your Microsoft Exchange 2010 Server, and at a command prompt, change the directory to the **inetsrv** folder:
   `cd c:\windows\system32\inetsrv`
2. At a command prompt, run the **appcmd** command using the new size limit value you entered in the previous section:
   `appcmd set config "Default Web Site/ews" -section:requestFiltering -requestLimits.maxAllowedContentLength:53600000`



```
c:\Windows\System32\inetsrv>appcmd set config "Default Web Site/ews" -section:re
questFiltering -requestLimits.maxAllowedContentLength:53600000
Applied configuration changes to section "system.webServer/security/requestFilte
ring" for "MACHINE/WEBROOT/APPHOST/Default Web Site/ews" at configuration commit
 path "MACHINE/WEBROOT/APPHOST/Default Web Site/ews"

c:\Windows\System32\inetsrv>
```

3. Close the command prompt.
4. Open **Services** and restart the following services:
    - Restart **IIS Admin Service**:



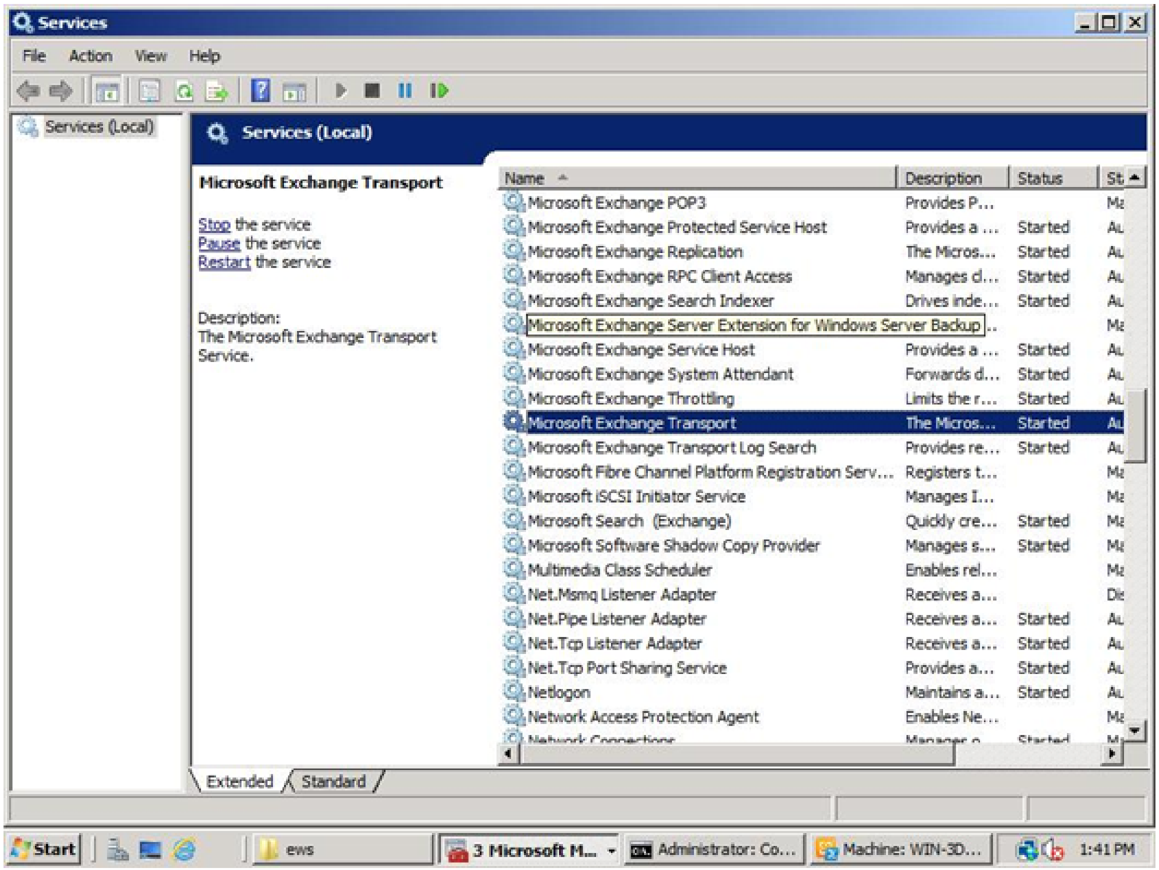
IIS Admin Service

Stop the service
Restart the service

Description:
Enables this server to administer the IIS metabase. The IIS metabase stores configuration for the SMTP and FTP services. If this service is stopped, the server will be unable to configure SMTP or FTP. If this service is disabled, any services that explicitly depend on it will fail to start.

Name	Description	Status	St
Function Discovery Resource Publication	Publishes t...	Started	Au
Group Policy Client	The servic...	Started	Au
Health Key and Certificate Management	Provides X....		Ma
Human Interface Device Access	Enables ge...		Ma
Hyper-V Data Exchange Service	Provides a ...	Started	Au
Hyper-V Guest Shutdown Service	Provides a ...	Started	Au
Hyper-V Heartbeat Service	Monitors th...	Started	Au
Hyper-V Time Synchronization Service	Synchroniz...	Started	Au
Hyper-V Volume Shadow Copy Requestor	Coordinate...	Started	Au
IIS Admin Service	Enables thi...	Started	Au
IKE and AuthIP IPsec Keying Modules	The IKEEX...	Started	Au
Interactive Services Detection	Enables us...		Ma
Internet Connection Sharing (ICS)	Provides n...		Di
IP Helper	Provides a...	Started	Au
IPsec Policy Agent	Internet Pr...	Started	Au
KtmRm for Distributed Transaction Coordinator	Coordinate...	Started	Au
Link-Layer Topology Discovery Mapper	Creates a ...		Ma
Microsoft .NET Framework NGEN v2.0.50727_X64	Microsoft		Di
Microsoft .NET Framework NGEN v2.0.50727_X86	Microsoft		Di
Microsoft .NET Framework NGEN v4.0.30319_X64	Microsoft		Au
Microsoft .NET Framework NGEN v4.0.30319_X86	Microsoft		Au
Microsoft Exchange Active Directory Topology	Provides A...	Started	Au

    - Restart **Microsoft Exchange Transport**:



Microsoft Exchange Transport

Stop the service
Pause the service
Restart the service

Description:
The Microsoft Exchange Transport Service.

Name	Description	Status	St
Microsoft Exchange POP3	Provides P...		Ma
Microsoft Exchange Protected Service Host	Provides a ...	Started	Au
Microsoft Exchange Replication	The Micros...	Started	Au
Microsoft Exchange RPC Client Access	Manages cl...	Started	Au
Microsoft Exchange Search Indexer	Drives inde...	Started	Au
Microsoft Exchange Server Extension for Windows Server Backup	..		Ma
Microsoft Exchange Service Host	Provides a ...	Started	Au
Microsoft Exchange System Attendant	Forwards d...	Started	Au
Microsoft Exchange Throttling	Limits the r...	Started	Au
Microsoft Exchange Transport	The Micros...	Started	Au
Microsoft Exchange Transport Log Search	Provides re...	Started	Au
Microsoft Fibre Channel Platform Registration Serv...	Registers t...		Ma
Microsoft iSCSI Initiator Service	Manages I...		Ma
Microsoft Search (Exchange)	Quickly cre...	Started	Ma
Microsoft Software Shadow Copy Provider	Manages s...	Started	Ma
Multimedia Class Scheduler	Enables rel...		Ma
Net.Msmq Listener Adapter	Receives a...		Di
Net.Pipe Listener Adapter	Receives a...	Started	Au
Net.Tcp Listener Adapter	Receives a...	Started	Au
Net.Tcp Port Sharing Service	Provides a...	Started	Au
Netlogon	Maintains a...	Started	Au
Network Access Protection Agent	Enables Ne...		Ma
Network Connections	Manages o...	Started	Ma

Barracuda Backup Restore

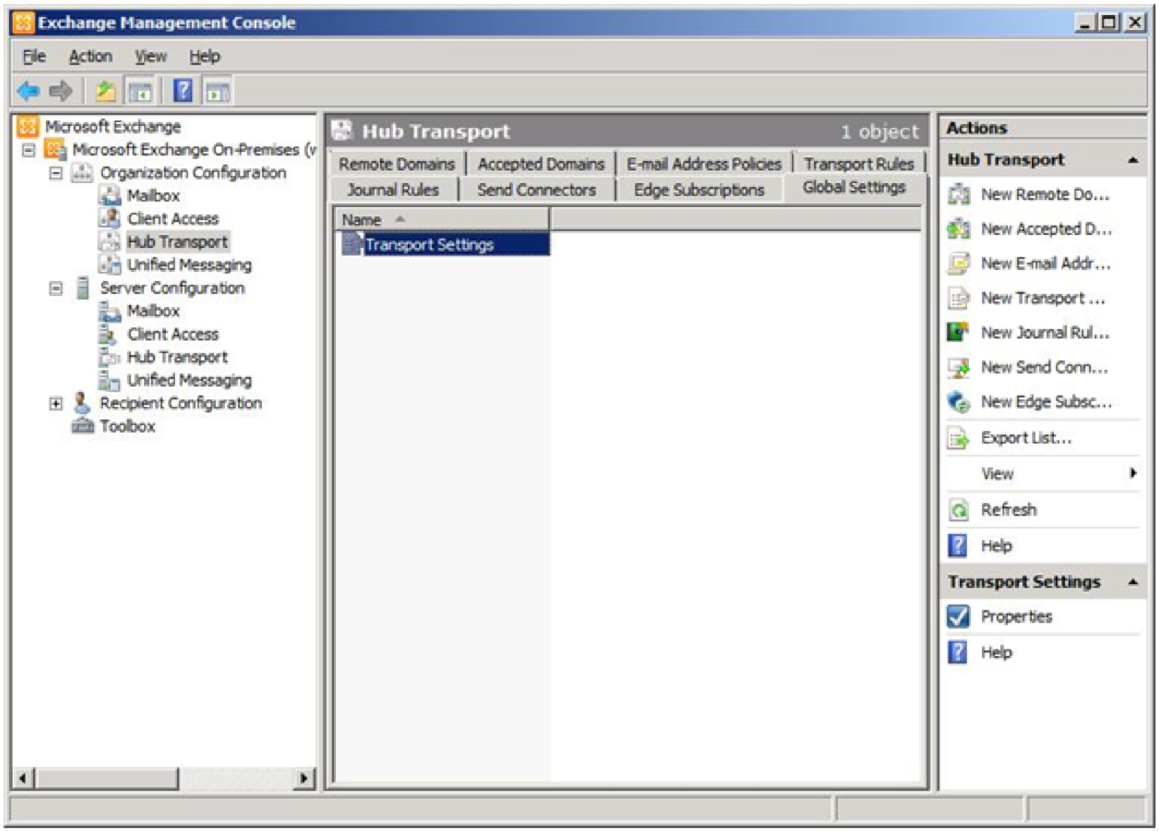
1. Log in to your Barracuda Backup web interface, and restore the messages that originally failed.
2. Messages should now restore without any errors. However, if you continue to encounter errors when restoring large messages, continue to the next section, Configuration Settings.

Configuration Settings

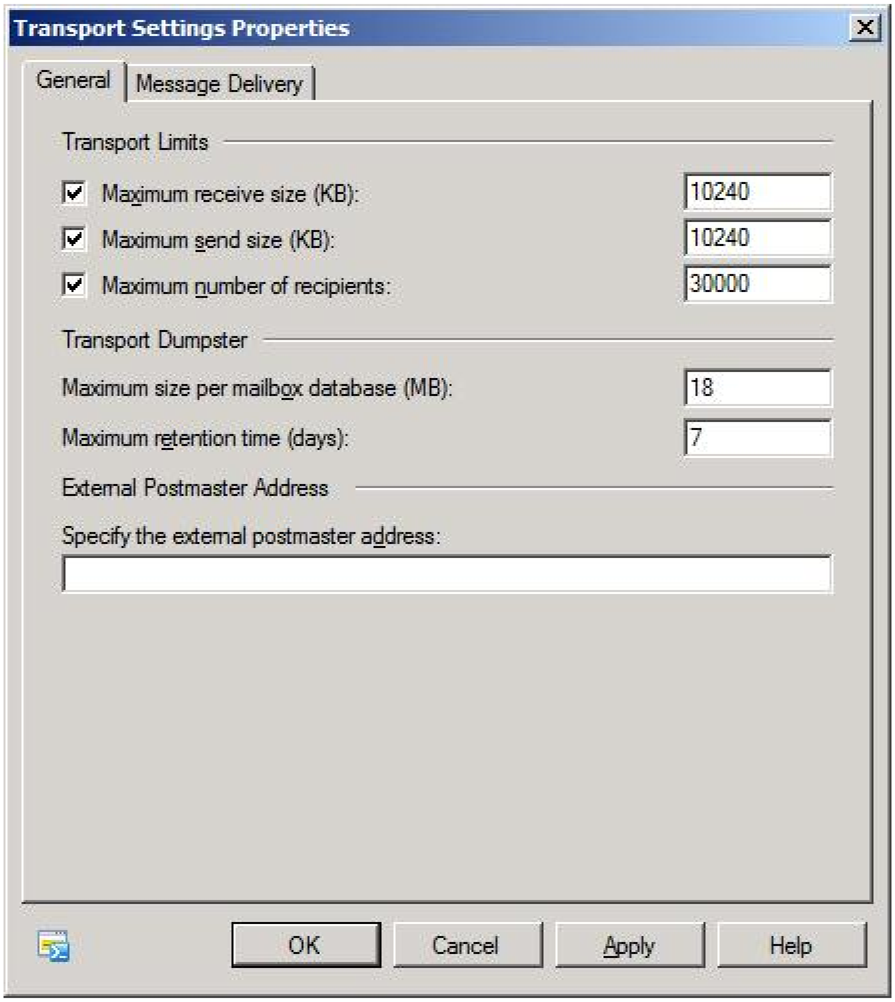
Microsoft Exchange 2010 Configuration Settings
Use the steps in the following sections *only* if you continue to encounter errors when restoring large messages.

Verify Exchange Management Console Settings

1. Log in to your Microsoft Exchange 2010 Server, and open the **Exchange Management Console (EMC)**.
2. Expand **Organization Configuration**, click **Hub Transport**, and click the **Global Settings** tab:


Exchange Management Console
File
Action
View
Help
Microsoft Exchange
Microsoft Exchange On-Premises (v
Organization Configuration
Mailbox
Client Access
Hub Transport
Unified Messaging
Server Configuration
Mailbox
Client Access
Hub Transport
Unified Messaging
Recipient Configuration
Toolbox
Hub Transport
1 object
Remote Domains
Accepted Domains
E-mail Address Policies
Transport Rules
Journal Rules
Send Connectors
Edge Subscriptions
Global Settings
Name
Transport Settings
Actions
Hub Transport
New Remote Do...
New Accepted D...
New E-mail Addr...
New Transport ...
New Journal Rul...
New Send Conn...
New Edge Subsc...
Export List...
View
Refresh
Help
Transport Settings
Properties
Help

3. Right-click **Transport Settings**, and click **Properties**:


Transport Settings Properties
General
Message Delivery
OK
Cancel
Apply
Help

Transport Limits

☑ Maximum receive size (KB): 10240

☑ Maximum send size (KB): 10240

☑ Maximum number of recipients: 30000

Transport Dumpster

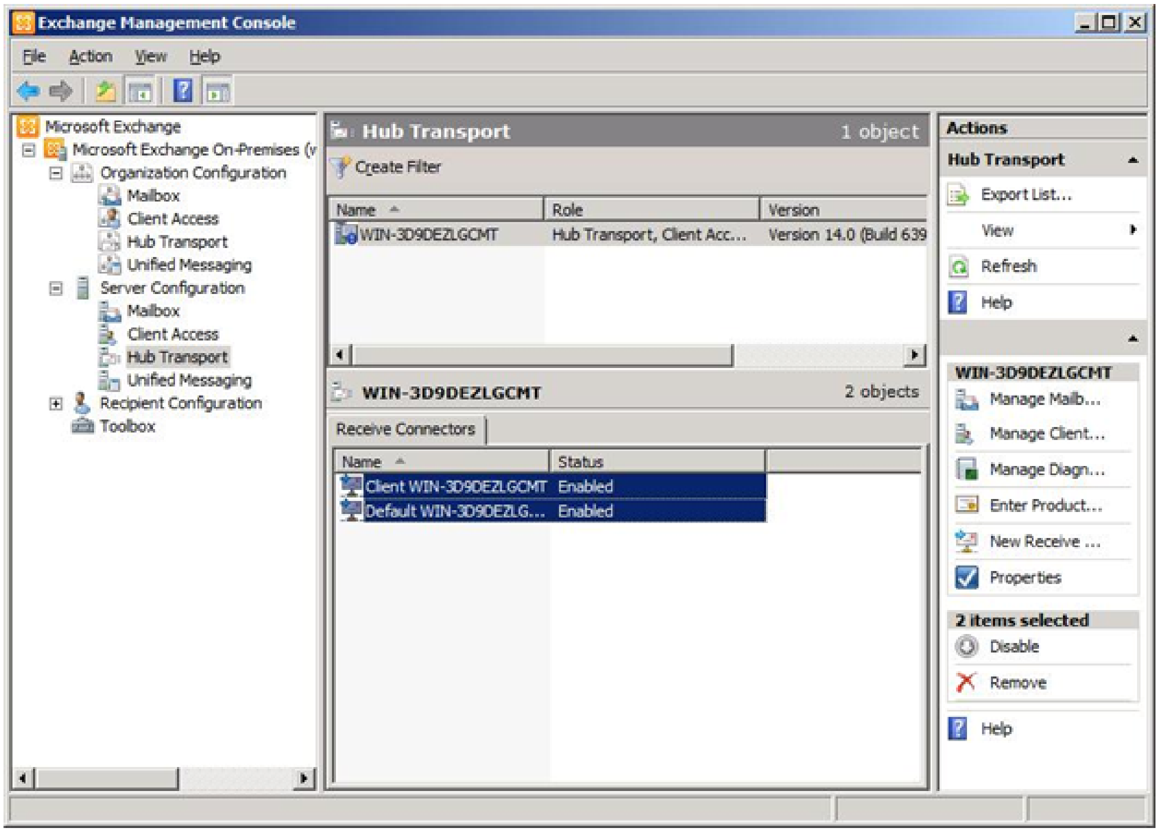
Maximum size per mailbox database (MB): 18

Maximum retention time (days): 7

External Postmaster Address

Specify the external postmaster address:

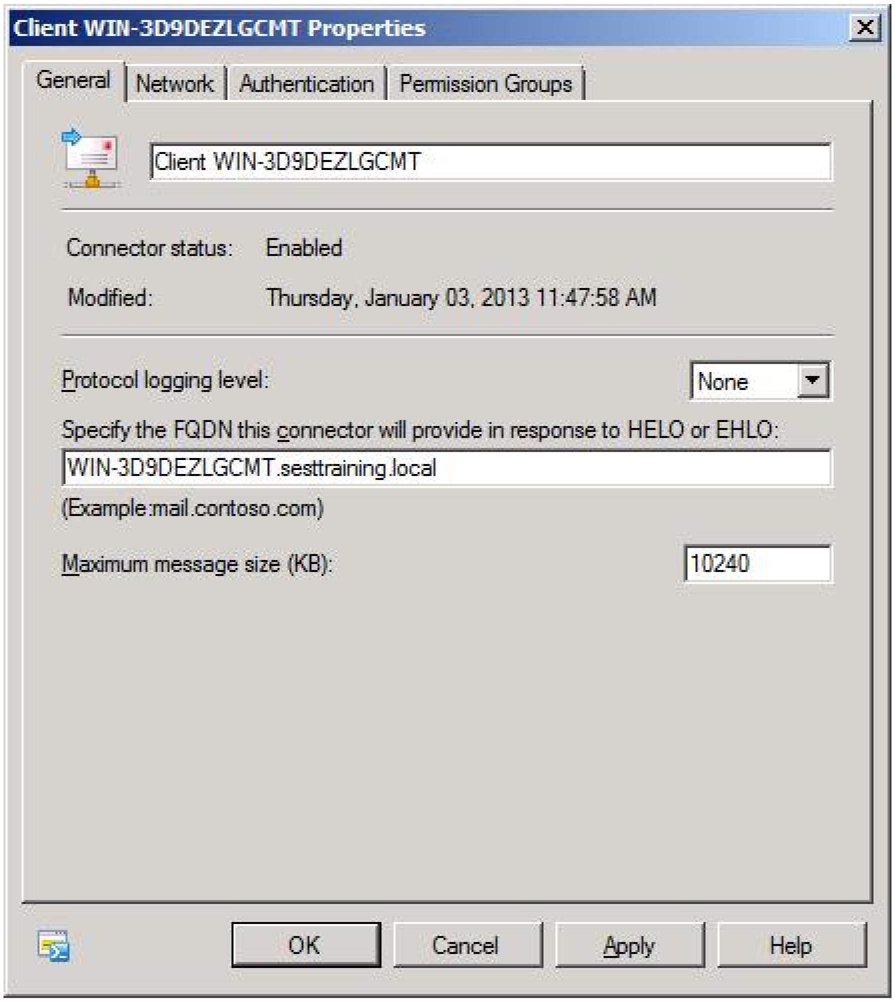
4. Verify the **Transport Limits** settings are large enough and listed correctly, then click **OK**.
5. In the **EMC**, expand **Server Configuration**, click **Hub Transport**:


Exchange Management Console
File
Action
View
Help
Microsoft Exchange
Microsoft Exchange On-Premises (v
Organization Configuration
Mailbox
Client Access
Hub Transport
Unified Messaging
Server Configuration
Mailbox
Client Access
Hub Transport
Unified Messaging
Recipient Configuration
Toolbox
Hub Transport
1 object
Create Filter
WIN-3D9DEZLGCMT
2 objects
Receive Connectors
Actions
Hub Transport
Export List...
View
Refresh
Help
WIN-3D9DEZLGCMT
Manage Mailb...
Manage Client...
Manage Diagn...
Enter Product...
New Receive ...
Properties
2 items selected
Disable
Remove
Help

Name	Role	Version
WIN-3D9DEZLGCMT	Hub Transport, Client Acc...	Version 14.0 (Build 639

Name	Status
Client WIN-3D9DEZLGCMT	Enabled
Default WIN-3D9DEZLG...	Enabled

6. Right-click on the **Client** Receive Connector, and click **Properties**:


Client WIN-3D9DEZLGCMT Properties
General
Network
Authentication
Permission Groups
OK
Cancel
Apply
Help

Client WIN-3D9DEZLGCMT

Connector status: Enabled

Modified: Thursday, January 03, 2013 11:47:58 AM

Protocol logging level: None

Specify the FQDN this connector will provide in response to HELO or EHLO: WIN-3D9DEZLGCMT.sesttraining.local

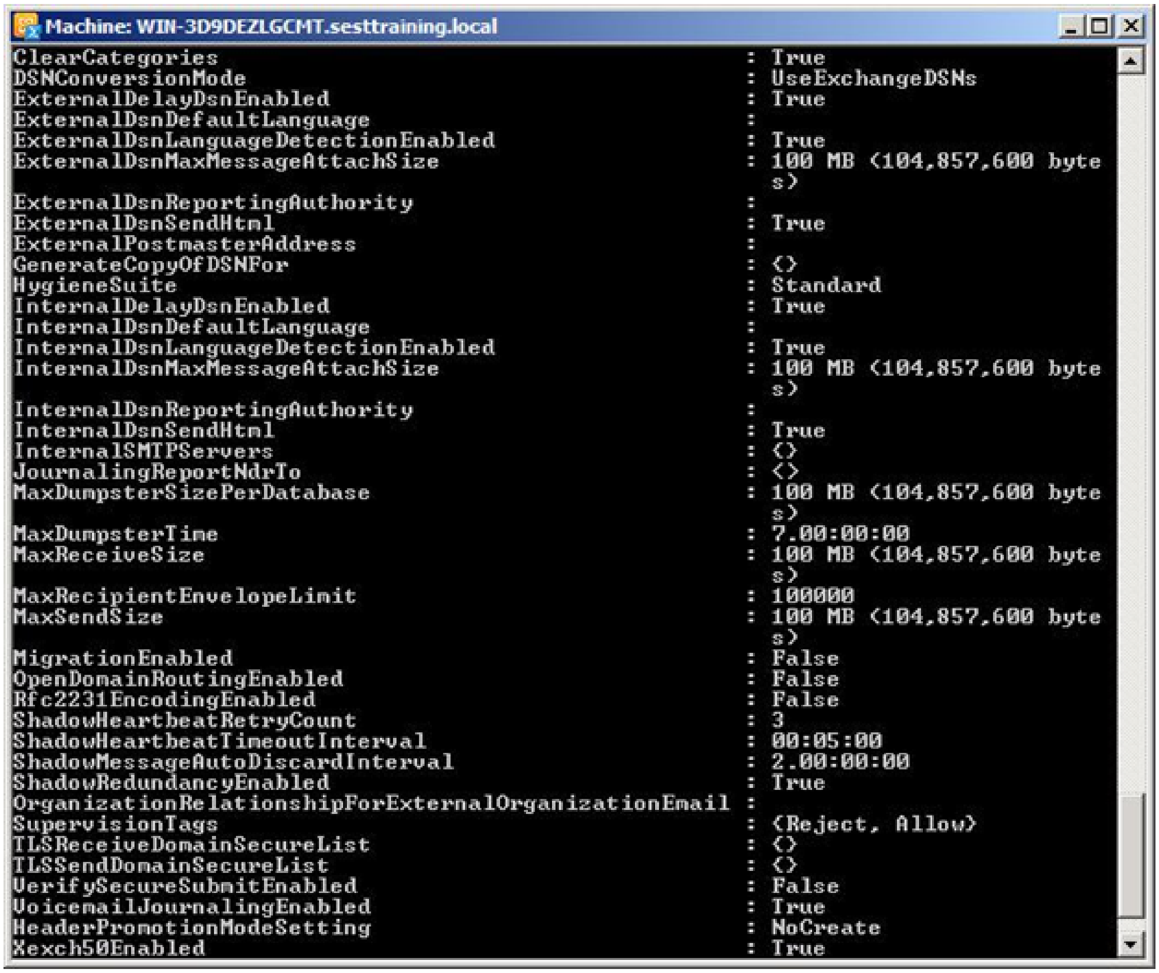
(Example:mail.contoso.com)

Maximum message size (KB): 10240

7. Verify the value in the **Maximum message size (KB)** is large enough to accommodate message restore.
8. Right-click the **Default** Receive Connector, click **Properties**, and verify the **Maximum message size (KB)** is large enough to accommodate message restore.
9. If you modified *any* settings in the preceding steps, go to **Services** and restart both **IIS Admin Service** and **Microsoft Exchange Transport** services.

Exchange Management Shell

1. Open the Exchange Management Shell, and enter the following command:
   `get-tranportconfig`:



```
ClearCategories                                      : True
DSNConversionMode                                    : UseExchangeDSNs
ExternalDelayDsnEnabled                              : True
ExternalDsnDefaultLanguage                           :
ExternalDsnLanguageDetectionEnabled                  : True
ExternalDsnMaxMessageAttachSize                      : 100 MB (104,857,600 byte
                                                       s)
ExternalDsnReportingAuthority                        :
ExternalDsnSendHtml                                  : True
ExternalPostmasterAddress                            :
GenerateCopyOfDSNFor                                 : {}
HygieneSuite                                         : Standard
InternalDelayDsnEnabled                              : True
InternalDsnDefaultLanguage                           :
InternalDsnLanguageDetectionEnabled                  : True
InternalDsnMaxMessageAttachSize                      : 100 MB (104,857,600 byte
                                                       s)
InternalDsnReportingAuthority                        :
InternalDsnSendHtml                                  : True
InternalSMTPServers                                  : {}
JournalingReportNdrTo                                : <>
MaxDumpsterSizePerDatabase                           : 100 MB (104,857,600 byte
                                                       s)
MaxDumpsterTime                                      : 7.00:00:00
MaxReceiveSize                                       : 100 MB (104,857,600 byte
                                                       s)
MaxRecipientEnvelopeLimit                            : 100000
MaxSendSize                                          : 100 MB (104,857,600 byte
                                                       s)
MigrationEnabled                                     : False
OpenDomainRoutingEnabled                             : False
Rfc2231EncodingEnabled                               : False
ShadowHeartbeatRetryCount                            : 3
ShadowHeartbeatTimeoutInterval                       : 00:05:00
ShadowMessageAutoDiscardInterval                     : 2.00:00:00
ShadowRedundancyEnabled                              : True
OrganizationRelationshipForExternalOrganizationEmail :
SupervisionTags                                      : {Reject, Allow}
TLSReceiveDomainSecureList                           : {}
TLSSendDomainSecureList                              : {}
VerifySecureSubmitEnabled                            : False
VoicemailJournalingEnabled                           : True
HeaderPromotionModeSetting                           : NoCreate
Xexch50Enabled                                       : True
```

2. Verify that the following settings are large enough and listed correctly:
   - `ExternalDsnMaxMessageAttachSize`
   - `InternalDsnMaxMessageAttachSize`
   - `MaxReceiveSize`
   - `MaxRecipientEnvelopeLimit (shown in KB)`
   - `MaxSendSize`
3. If any of the values need modification, run the following command:
   `Set-transportconfig -<`*`setting to be changed`*`> <`*`size`*`>`
   For example:
   `set-transportconfig -MaxSendSize 50MB`
4. If you modified *any* values through the Exchange Management Shell, go to **Services** and restart both **IIS Admin Service** and **Microsoft Exchange Transport** services.

How to Resolve Snapshot Backup Errors

> This article refers to Barracuda Backup firmware version 5.0 or higher, and Microsoft® Windows Server 2003, Windows Vista, Windows 7, and Windows 2008, except where noted.

If you receive a **File System Snapshot was Released** reporting error, a partition may be heavily used or fragmented. Use the steps in this article to determine the issue and to resolve the error on the Windows 2003 Server.

In this article:

- Determine the Source of the Issue
- Move the Snapshot Location
- Defragmentation
- Verify Service Packs and Patches are Installed

Determine the Source of the Issue

Windows Server 2003
This step applies to Windows Server 2003 only.

Determine the source of the issue is to identify the partition causing the problem. To do so, complete the following steps:

1. Go to the system even log on the server in question.
2. Look for an event with the source `volsnap` and an id of `25/35` containing the following message:

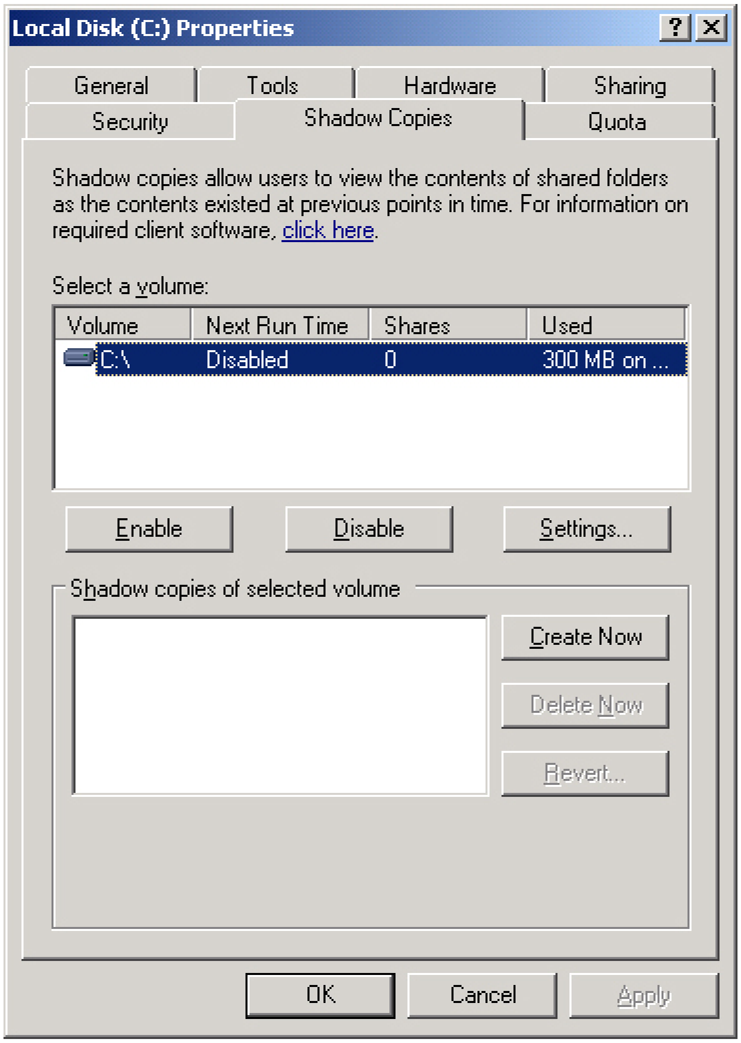
```
The shadow copies of volume volume name were aborted because the diff area file could not grow in
time. Consider reducing the IO load on this system to avoid this problem in the future.
```

Move the Snapshot Location

This step applies to Windows 2003, Windows Vista, Windows 7, and Windows 2008.

First determine if the server has multiple partitions with available disk space, and then move the snapshot location to a less used disk using the following steps:

1. On a Microsoft 2003 Server, log into the server as the administrator, go to **My Computer**, and right-click on the troubled partition.
2. Select **Properties**, and click the **Shadow Copies** tab:



Local Disk (C:) Properties

General
Tools
Hardware
Sharing
Security
Shadow Copies
Quota

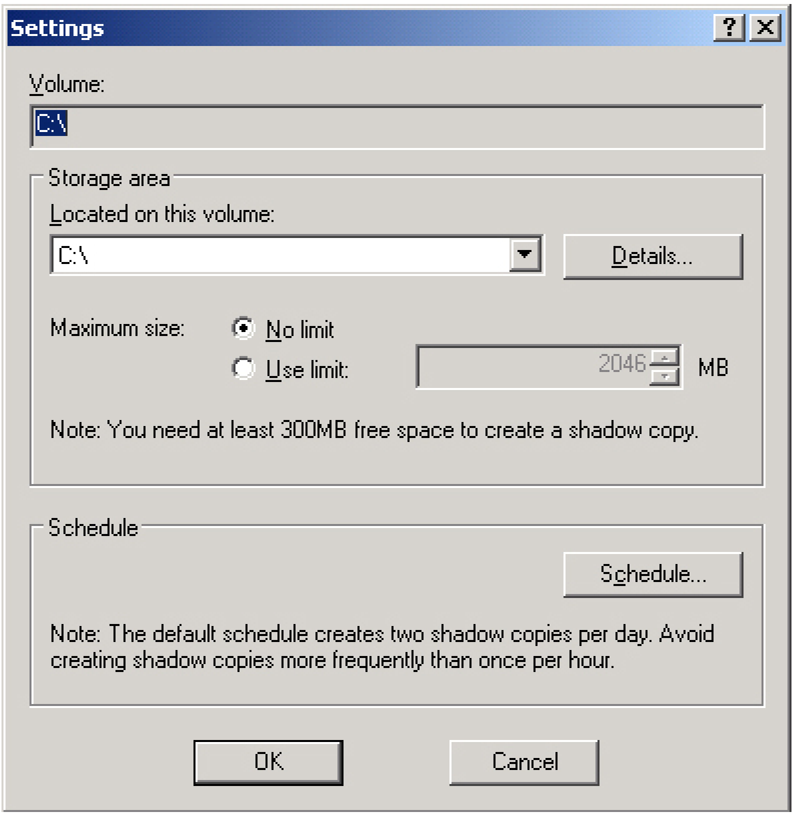
Shadow copies allow users to view the contents of shared folders as the contents existed at previous points in time. For information on required client software, click here.

Select a volume:

Volume	Next Run Time	Shares	Used
C:\	Disabled	0	300 MB on ...

Enable
Disable
Settings...
Shadow copies of selected volume
Create Now
Delete Now
Revert...
OK
Cancel
Apply

3. In the **Select a volume** list, click on the troubled partition, and click **Settings**:


Settings
Details...
Schedule...
OK
Cancel

Volume: C:\

Storage area

Located on this volume: C:\

Maximum size: ● No limit ○ Use limit: 2046 MB

Note: You need at least 300MB free space to create a shadow copy.

Schedule

Note: The default schedule creates two shadow copies per day. Avoid creating shadow copies more frequently than once per hour.

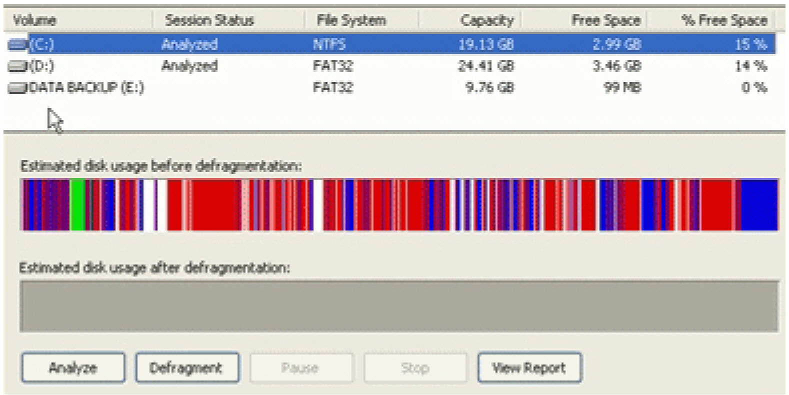
4. In the **Settings** dialog box, from the **Located on this volume** drop-down menu select a partition with available space, and then click **OK**.

> ⓘ Verify the maximum size is adequate to back up the partition.

Defragmentation

> ⓘ This step applies to Windows 2003, Windows Vista, Windows 7, and Windows 2008.

Analyze the partition in question for a Defrag. The disk will show up heavily fragmented:


Estimated disk usage before defragmentation:
Estimated disk usage after defragmentation:
Analyze
Defragment
Pause
Stop
View Report

Volume	Session Status	File System	Capacity	Free Space	% Free Space
(C:)	Analyzed	NTFS	19.13 GB	2.99 GB	15 %
(D:)	Analyzed	FAT32	24.41 GB	3.46 GB	14 %
DATA BACKUP (E:)		FAT32	9.76 GB	99 MB	0 %

> ⓘ It is recommended that you defragment the hard drive during off hours in order to reduce server load during normal business hours.

Verify Service Packs and Patches are Installed

Windows Server 2003
This step applies to Windows 2003 *only*.

Verify that both the server and snapshot instance have all service packs and patches installed, and then use the following steps to adjust the page file to 1.5 of the amount of RAM:

1. Log into the server as the administrator, and open **System** in the **Control Panel**.
2. On the **Advanced** tab, in the **Performance** section, click **Settings**.
3. In the **Virtual Memory** section, click **Change**.
4. Under **Drive [Volume Label]**, click the drive containing the paging file you want to change.
5. In the **Paging file size for selected drive** section, click **Custom size**, and type a new paging file size in megabytes in the **Initial size (MB) or Maximum size (MB)** field; click **Set**.

If you decrease the size of either the initial or maximum page file settings, you must restart your computer to see the effects of those changes. Increases typically do not require a system restart. For additional information, refer to the Microsoft solution

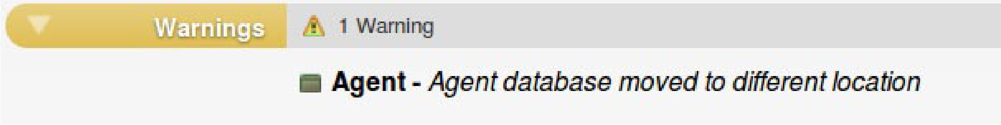
For Windows Server 2003, you can apply these roll-ups supplied by Microsoft to solve this problem; note that you must restart after applying a roll-up. Each patch should be applied individually and a backup run after the patch is applied to see if this resolves the issue:

- http://support.microsoft.com/kb/940349
- http://support.microsoft.com/kb/979457
- http://support.microsoft.com/kb/943669
- http://support.microsoft.com/kb/981166

Resolving "Agent database moved to different location" Warning

The Barracuda Backup Agent requires at least 1GB of free disk space on a data source for its database. If less than the required amount of disk space is available, the Barracuda Agent database is automatically moved to another storage volume.

While backups will continue to run, a warning message displays in the Barracuda Backup web interface stating that the database has been moved:



Agent - *Agent database moved to different location*

To resolve this issue, install the Barracuda Backup Agent to an alternate storage volume with adequate free disk space.

Updating the Backup Agent Location

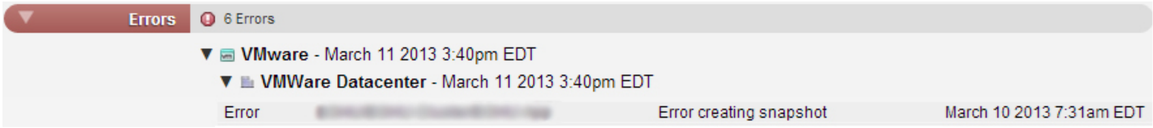
Use the following steps to move the Barracuda Backup Agent to an alternate storage volume and eliminate the warning message:

1. Completely uninstall the Barracuda Backup Agent using the **Add/Remove Programs** or **Programs and Features** option on your system.
2. Once the Agent is uninstalled, log in to the Barracuda Backup web interface, and go to the **SUPPORT > Software Downloads** page.
3. Download and install the latest version of the Barracuda Backup Agent.
4. During installation, select the installation path on a storage volume with at least 1GB of free disk space.
5. Once the next successful backup occurs, the warning message no longer displays.

Resolving "Error Creating Snapshot" Error During ESX/ESXi Virtual Machine Backup

This article refers to all Barracuda Backup firmware 5.0 and higher, and VMware® 4.0 and above with the VMware license which includes access to vSphere® Data Recovery API.

This article describes how to resolve the error "Error creating snapshot" encountered while backing up an ESX/ESXi virtual machine, as shown in the following image:



▼ **VMware** - March 11 2013 3:40pm EDT
▼ **VMWare Datacenter** - March 11 2013 3:40pm EDT
Error [redacted] Error creating snapshot March 10 2013 7:31am EDT

The most common causes for this error are the size of the snapshot being created is larger than the available free space on the datastore, or a vss writer error.

Additional Information
For more information, refer to the following VMware knowledgebase articles:

- VMware Data Recovery backup fails with the error: Failed to create snapshot. Error -3941 (1028924)
- Cannot create a quiesced snapshot because the snapshot operation exceeded the time limit for holding off I/O in the frozen virtual machine (1018194)

Resolving "Error Reading Object" Error During ESX or ESXi Virtual Machine Backup

This article refers to all Barracuda Backup firmware 5.0 and higher, and VMware® 4.0 and above with the VMware license which includes access to vSphere ® Data Recovery API .

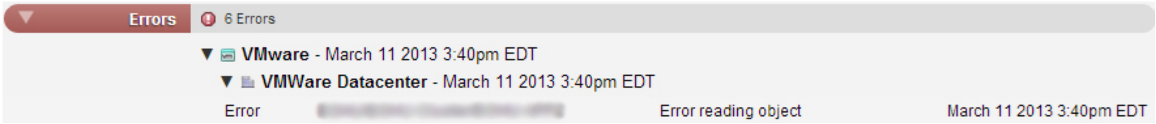
Additional Resource
VMware knowledgebase: QueryChangedDiskAreas API call returns a FileFault error (2035976)

This article describes how to resolve the error "Error reading object" encountered while backing up an ESX/ESXi virtual machine. The most common causes for this error are a crashed virtual machine or missing blocks on the virtual machine. When an error is encountered when backup up the disk, the following displays in the vSphere logs:

```
Error QueryChangedDiskAreas
```

Contact Barracuda Networks Technical Support for information on enabling CBT from the VMware API.

If you receive this error:



Errors 6 Errors
▼ VMware - March 11 2013 3:40pm EDT
▼ VMWare Datacenter - March 11 2013 3:40pm EDT
Error [redacted] Error reading object March 11 2013 3:40pm EDT

Use the following steps to resolve this error:

1. Remove all virtual machine snapshots.
2. Disable changed block tracking.
3. Enable changed block tracking.

Resolving "Error Removing Snapshot" Error During ESX/ESXi Virtual Machine Backup

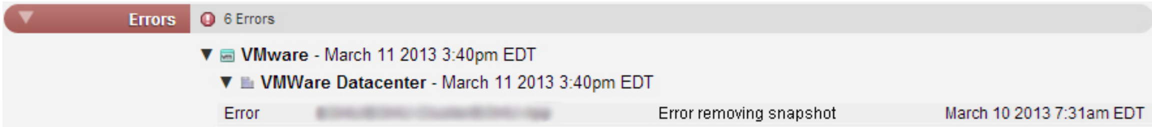
This article refers to Barracuda Backup firmware version 3.0 and higher, VMware® 4.0 and above, VMware vCenter, vSphere®, and ESX, and Agent for VMware Virtual Infrastructure (AVVI).

When AVVI is enabled, you cannot manually delete a vCenter snapshot because when a snapshot is removed from a virtual machine, ESX automatically creates a Consolidated Helper-0 snapshot which holds the snapshot data until the actual snapshot is deleted. Once the process is complete, the Consolidated Helper-0 is rolled into the resulting **.vmdk** file only when the following conditions are met:

- Consolidated Helper-0 snapshot file size must meet the minimal snapshot size in VMware which is less than 16MB
- None or minimal I/O write on the virtual machine

To automatically delete a vCenter snapshots, log into the Barracuda Backup web interface, and go to the **BACKUP > Schedules** page.

If you attempt to manually delete a vCenter snapshot from Barracuda Backup before the Consolidated Helper-0 snapshot is rolled into the VMDK, an error displays in the **REPORTS > Backup** report page in the Barracuda Backup web interface, as shown in the following image:



VMware - March 11 2013 3:40pm EDT

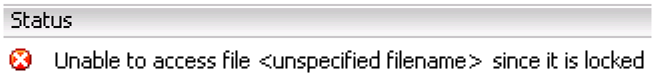
VMWare Datacenter - March 11 2013 3:40pm EDT

Error [redacted] Error removing snapshot March 10 2013 7:31am EDT

Verifying VMware Disk I/O Issues

If you continue to encounter an error, you may wish to confirm whether there are I/O issues on the virtual machine causing high CPU usage.

1. Log into and restart the virtual machine to commit the Consolidated Helper-0 snapshot.
2. Log into the vCenter/vSphere Snapshot Manager and create a **quiesce** snapshot file.
3. Once the **quiesce** snapshot is created, click on the **quiesce** snapshot file name, and click **Delete**.
4. When you delete the snapshot, if a Consolidate Helper-0 snapshot continues to display, and the **Status** field displays an error message similar to the following:



Unable to access file <unspecified filename> since it is locked

You may need to adjust your virtual environment to resolve the high CPU usage.

How to Unlock the quiesce Snapshot

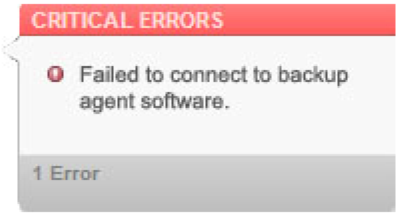
Use the following steps to unlock the Consolidated Helper-0 file:

1. Log into and restart the virtual machine.
2. Allow the **quiesce** snapshot to commit the snapshot; the Consolidated Helper-0 file should be automatically removed once this process is complete.

Resolving "Failed to connect to backup agent software" Error

This article refers to all Barracuda Backup firmware 5.0 and higher, and the Barracuda Backup Agent.

The Barracuda Agent is a light weight agent that performs source side-based deduplication, and securely transfers changes over port 5120. Use the following steps to resolve the "Failed to connect to backup agent software" error:



Failed to connect to backup agent software.

Step 1. Verify Barracuda Backup Agent is Started

1. Log in to the Barracuda Backup web interface, and go to the **BACKUP > Data Sources** page.
2. Determine which Server is unable to connect to the Backup Agent.
3. Log in to that Server, open Services, and verify that the Barracuda Backup Agent Service is started.
4. If the Service is not started, restart it.

If you are still unable to connect to the Agent, move on to the next step.

Step 2. Verify Windows Firewall Rules

If you are running Windows Firewall, make sure that you have both an inbound and an outbound rule created and enabled for Barracuda Backup.

1. Log in to Windows Firewall, and click **Inbound Rules** in the left pane.
2. If a rule for Barracuda Backup is listed in the center pane, right-click the rule and verify it is enabled.
3. If there is *not* a rule, create and enable a rule for Barracuda Backup.
4. In the left pane, click **Outbound Rules**; complete steps **2** and **3** for the outbound rule.

Step 3. Ping Barracuda Backup from the Server

You can use the **ping** command to check whether the Barracuda Backup IP address is accessible from the Server.

1. Log in to the Server that is unable to connect to the Backup Agent.

2. Ping the IP address of the Barracuda Backup Server.

For additional information and ping command options, refer to the Microsoft TechNet article Using the ping command.

Step 4. Test and Reinstall Barracuda Backup Agent

1. Log in to Barracuda Backup and download and install the latest Barracuda Agent from the **SYSTEM > Software Downloads** page.
2. Once the Agent is installed, go to the **BACKUP > Data Sources** page.
3. To the right of the Server unable to connect, click **Verify connectivity with the Barracuda Backup Agent software**.
4. In the **Edit Server** page, click **Test Software Connectivity**.

If you are still unable to connect to the Agent, move on to the next step.

Resolving "File System Snapshot was Released" Error

This article refers to all Barracuda Backup firmware versions, and Microsoft® Windows® 2003 Server.

If you receive a **File System Snapshot was Released** reporting error, a partition may be heavily used or fragmented. Take the following steps to determine the issue and to resolve the error on the Windows 2003 Server.

Step 1. Determine the Source of the Issue

The first step in determining the source of the issue is to identify the partition causing the problem. To do so, complete the following steps:

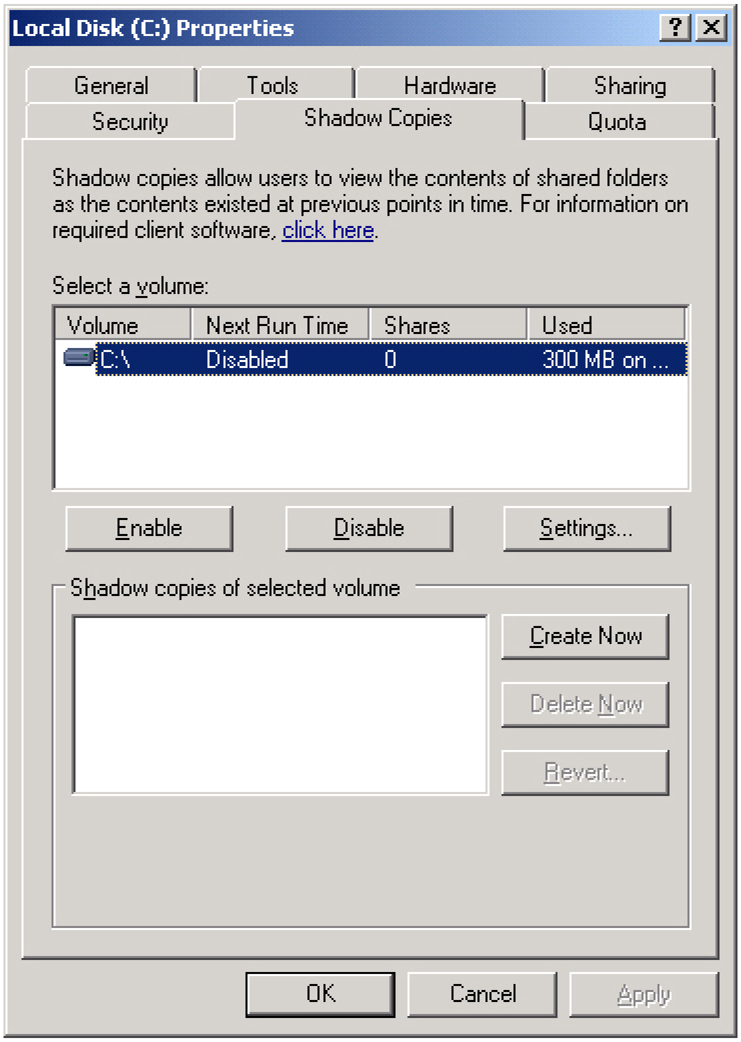
1. Go to the system even log on the server in question.
2. Look for an event with the source `volsnap` and an id of `25/35` containing the following message:

```
The shadow copies of volume <volume name> were aborted because the diff area file could not grow in
time. Consider reducing the IO load on this system to avoid this problem in the future.
```

Step 2. Move the Snapshot Location

First determine if the server has multiple partitions with available disk space, and then move the snapshot location to a less used disk using the following steps:

1. On a Microsoft 2003 Server, log into the server as the administrator, go to **My Computer**, and right-click on the troubled partition.
2. Select **Properties**, and click the **Shadow Copies** tab:

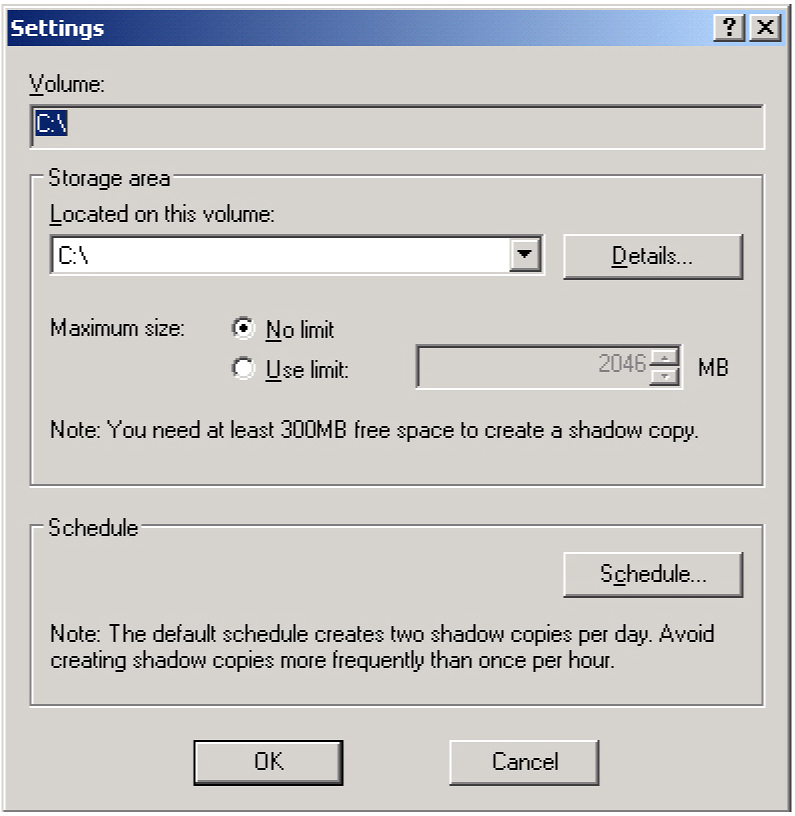

Local Disk (C:) Properties
General
Tools
Hardware
Sharing
Security
Shadow Copies
Quota
Enable
Disable
Settings...
Shadow copies of selected volume
Create Now
Delete Now
Revert...
OK
Cancel
Apply

Shadow copies allow users to view the contents of shared folders as the contents existed at previous points in time. For information on required client software, click here.

Select a volume:

Volume	Next Run Time	Shares	Used
C:\	Disabled	0	300 MB on ...

3. In the **Select a volume** list, click on the troubled partition, and click **Settings**:


Settings
?
Storage area
Details...
Schedule
Schedule...
OK
Cancel

Volume: C:\

Located on this volume: C:\

Maximum size: ● No limit ○ Use limit: 2046 MB

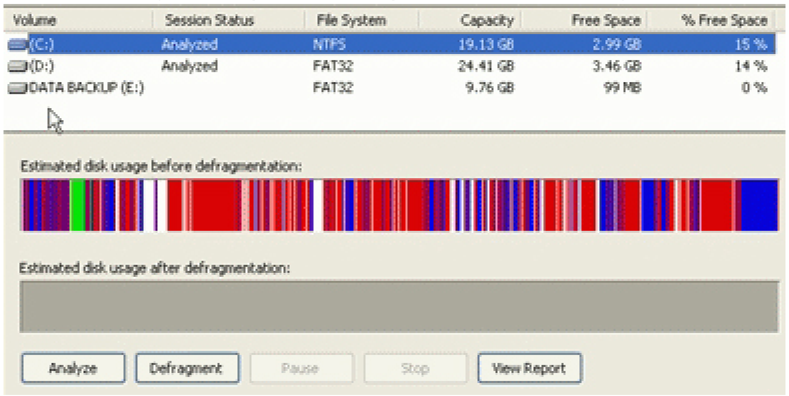
Note: You need at least 300MB free space to create a shadow copy.

Note: The default schedule creates two shadow copies per day. Avoid creating shadow copies more frequently than once per hour.

4. In the **Settings** dialog box, from the **Located on this volume** drop-down menu select a partition with available space, and then click **OK**.

> Verify the maximum size is adequate to back up the partition.

Second, analyze the partition in question for a Defrag. The disk will show up heavily fragmented:



Volume	Session Status	File System	Capacity	Free Space	% Free Space
(C:)	Analyzed	NTFS	19.13 GB	2.99 GB	15 %
(D:)	Analyzed	FAT32	24.41 GB	3.46 GB	14 %
DATA BACKUP (E:)		FAT32	9.76 GB	99 MB	0 %

Estimated disk usage before defragmentation:
Estimated disk usage after defragmentation:
Analyze
Defragment
Pause
Stop
View Report

> It is recommended that you defragment the hard drive during off hours in order to reduce server load during normal business hours

Additional Information

If these solutions do not work make sure the customer is updated to the latest service pack.

For Windows 2003 Servers, you can apply these roll-ups supplied by Microsoft to solve this problem; note that you must restart after applying a roll-up. Each patch should be applied individually and a backup run after the patch is applied to see if this resolves the issue:

- http://support.microsoft.com/kb/940349
- http://support.microsoft.com/kb/979457
- http://support.microsoft.com/kb/943669
- http://support.microsoft.com/kb/981166

Resolving "Incremental backups cannot be performed while circular logging is enabled" Error

This article refers to all Barracuda Backup firmware, and Microsoft® Exchange Server 2003, 2007, 2010, or 2013; note that circular logging is disabled by default in Microsoft Exchange 2010 and 2013.

In this article:

- Logging Cycle
- Disable Circular Logging in Exchange 2003
- Disable Circular Logging in Exchange 2007
- Disable Circular Logging in Exchange 2010
- Disable Circular Logging in Exchange 2013

Logging Cycle

Circular Logging is designed to save storage on your Microsoft Exchange Server by preventing transaction logs from building up on the Server. This is achieved by creating and writing to a total of four transaction log files. Once the fourth log is full, it cycles back to the first log and overwrites it, creating a logging cycle referred to as "Circular Logging." Once the first log is full, it then moves on to overwrite the second, third, and fourth, and then cycles back to the first log. The assumption is that by the time the fourth log is filled, the first log is committed.

These transaction logs are saved for use when restoring data. If Circular Logging is enabled, this is not possible as you are able to restore only to the last full backup as the transaction log sequence is not consistent making it unreliable.

If you are unable to complete a Smart Backup or Log Backup of your Microsoft Exchange Server, Circular Logging may be enabled. In this case, an error similar to the following displays either in the Barracuda Backup web interface or in a Barracuda Backup report:

> **Incremental backups cannot be performed while circular logging is enabled for *<Exchange Storage Group>*. Disable circular logging to perform incremental backups.**

Disable Circular Logging in Exchange 2003

Use the following steps to disable circular logging for the Exchange Storage Groups on the Exchange Server 2003:

1. Log into the Exchange Server as the administrator, and go to **Start > Programs > Microsoft Exchange > System Manager**.
2. In the console tree, expand **Server**, right-click the storage group, and click **Properties**.
3. In the **Properties** dialog box, turn *Off* **Enable circular logging**, and click **OK**.
4. Click **Yes** to confirm you want to continue and close the **Properties** dialog box.
5. Go to **Start > Programs > Administrative Tools > Services**.
6. In the right pane, click **Microsoft Exchange Information Store**, and click **Restart** in the **Action** menu.
7. Click **Yes** to restart the service.

Disable Circular Logging in Exchange 2007

Use the following steps to disable circular logging for the Exchange Storage Groups on the Exchange Server 2007:

1. Log into the Exchange Server as the administrator, and open the Exchange Management Console (EMC).
2. In the console tree, expand **Server Configuration**, and click **Mailbox**.
3. In the center pane, right-click the storage group for which you want to disable Circular Logging, and click **Properties**.
4. The **Storage Group Properties** dialog box displays. Turn *Off* **Enable circular logging**, and click **OK** to close the **Properties** dialog box.
5. Restart the Microsoft Exchange Information Store service or dismount and then mount all of the databases in the storage group.

Disable Circular Logging in Exchange 2010

Circular logging is disabled by default in Microsoft Exchange 2010.

Use the following steps to disable circular logging for the Exchange Storage Groups on the Exchange Server 2010:

1. Log into the Exchange Server as the administrator, and open the Exchange Management Console (EMC).
2. In the console tree, expand **Organization Configuration**, and click **Mailbox**.
3. In the result pane, click the **Database Management** tab and click **Properties** below the storage group database.
4. Click the **Maintenance** tab, and turn *Off* **Enable circular logging**. Click **OK** to close the **Properties** dialog box.
5. Restart the Microsoft Exchange Information Store service or dismount and then mount all of the databases in the storage group.

Disable Circular Logging in Exchange 2013

> Circular logging is disabled by default in Microsoft Exchange 2013.

Use the following steps to disable circular logging for the Exchange Storage Groups on the Exchange Server 2013:

1. Log into the Exchange Server as the administrator.
2. In the left pane, click **servers**, and then click **databases** at the top of the page.
3. Click on the Mailbox Database, and click the **edit** (✎) icon.
4. In the **Properties** window, click **maintenance**, and turn *Off* **Enable circular logging**.
5. Click **save** to close the **Properties** window.
6. Click on the Mailbox Database once again, and click the **more** (•••) icon.
7. Click **Dismount database**. Once the view refreshes, click the **more** (•••) icon once again, and click **Mount database**.

> Before you can complete an Exchange Server Smart Backup or Log Backup, you must first perform a full backup to ensure that transaction logs are reset.

Resolving “An error occurred during agent backup initialization" Error

> This article refers to Barracuda Backup firmware version 5.0 or higher.

In this article:

- View Data Source Errors
- Review Reports
- Review Backup Agent Log Files
- Review Source Logs

If a backup fails, and the error "An error occurred during backup initialization" displays, there can be a number of causes. Use the information in this article to resolve this error.

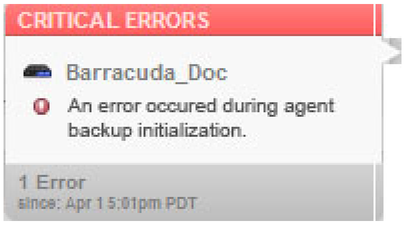
> You may need the Barracuda Backup Agent log files and Server Application and System log files to assist in troubleshooting this error.

Use the following troubleshooting options to resolve this error:

- Review error message details on the data source
- Review the Barracuda Backup Reports
- Review the Backup Agent **bbtrace.txt** log file
- Review the Server Application and System event logs
- Additional resources

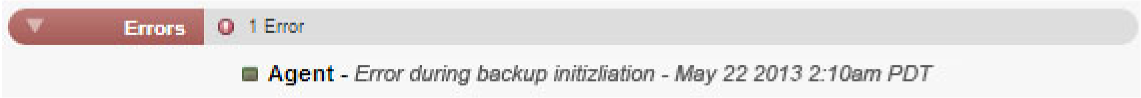
> If you receive an email report stating that a source has failed to back up data, or if you notice a red status indicator in the **STATUS** page , use these steps to determine the cause of the error.

View Data Source Errors

1. Log in to Barracuda Backup, and go to the **BACKUP > Sources** page.
2. To the right of the source, a red status indicator (🟥) displays if an error is generated during backup. Mouse-over the status indicator to view a pop-up message describing the cause of the error:

CRITICAL ERRORS
Barracuda_Doc
An error occured during agent backup initialization.
1 Error
since: Apr 1 5:01pm PDT
3. If the error "An error occurred during agent backup initialization" displays, then something during the beginning of the Agent backup failed.

Review Reports

Use the following steps to review the Barracuda Backup Agent log file and determine if something failed to initialize.

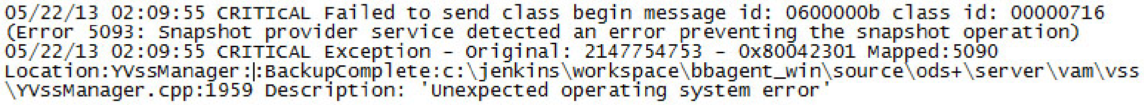
1. Go to the **REPORTS > Backup** page, and select the following options in the filter section above the table:
    a. **Schedules** - Select **All**
    b. **Sources** - Select **Agent** directly below the Source in question
    c. **From** - Specify a date
2. View the list of reports. A red status indicator displays to the left of a failed backup. Click **Details** to the right of the most recent backup report.
3. At the bottom of the **Report** details page, a list of errors display. Determine the date and time the error occurred:

Errors 1 Error
Agent - *Error during backup initizliation - May 22 2013 2:10am PDT*

Review Backup Agent Log Files

Use these steps to review the Backup Agent log files for the specific error reported by the Backup Agent.

1. Log in to the data source that is failing to back up data, and go to the Backup Agent log files. By default, the log files are located in:
   C:\Program Files\Barracuda\Barracuda Backup Agent\log
2. Locate the file **bbtrace.txt**; this is the most recent log file.

> ⓘ If the server was rebooted, or the agent was restarted, you may need to review older **bbtrace.txt** files to find the time listed in the **Report** details page in the previous step.

3. Open **bbtrace.txt** in Notepad. This file contains data that is helpful in determining the specific error. Each log entry is time stamped, so you will first want to identify when the failed backup occurred based on the **Report** details page; note that there may be multiple days of log details so it is recommended that you use the search function to find the error.
4. Search the log file for terms such as **Failed** or **Critical**. Once you locate the term, review the associated content to determine the specific error message:

```
05/22/13 02:09:55 CRITICAL Failed to send class begin message id: 0600000b class id: 00000716
(Error 5093: Snapshot provider service detected an error preventing the snapshot operation)
05/22/13 02:09:55 CRITICAL Exception - Original: 2147754753 - 0x80042301 Mapped:5090
Location:YVssManager:|:BackupComplete:c:\jenkins\workspace\bbagent_win\source\ods+\server\vam\vss
\YVssManager.cpp:1959 Description: 'Unexpected operating system error'
```
In this example, a VSS snapshot failed due to an unexpected operating system error on the targeted server.

> ⓘ Note that an Agent error message is typically followed by associated `CRITICAL Sup: Resource not put` details which is not needed for troubleshooting.

Review Source Logs

If the Backup Agent log files indicate an error on the source, use the following steps to review the Application and System log files:

1. Log in to the source server, and locate the Application and System log files for further troubleshooting.
2. In the Application and System log files, locate the time the errors occurred on the Backup Agent based on the **Report** details page.
3. Critical errors should display for the time in the log files.
4. Review the error messages and determine if additional troubleshooting is needed on the source.

> ⓘ Review the error messages and determine if additional troubleshooting is needed on the source. Use the event ID found in the Application and System event log files, and use an Internet search engine for troubleshooting.

Resolving "Unable to back up virtual machines with independent disks" Error

> This article refers to Barracuda Backup firmware version 5.0 and higher, and VMware® 4.0 and above with the VMware license which includes access to vSphere® Data Recovery API.

Related Articles

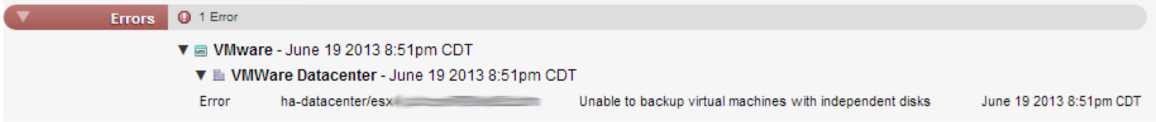
- Resolving "Error Creating snapshot"- ESX/ESXi VM Backup

Additional Resource

- Understanding virtual machine snapshots in VMware ESX
- Creating a virtual machine snapshot fails with the error: The attempted operation cannot be performed in the current state (Powered Off)
- Taking a snapshot with virtual machine memory stuns the virtual machine while the memory is written to disk

Use the steps in this article to resolve the "Unable to back up virtual machines with independent disks" error while backing up an ESX/ESXi virtual machine.

If you encounter the following error while backing up an ESX/ESXi virtual machine:



VMware - June 19 2013 8:51pm CDT

VMWare Datacenter - June 19 2013 8:51pm CDT

Error ha-datacenter/esx[redacted] Unable to backup virtual machines with independent disks June 19 2013 8:51pm CDT

When you revert a virtual machine snapshot, it returns to the state the system was in when the snapshot was taken by reloading the memory and eliminating the matching disk snapshot. However, VMware does not support snapshots of independent disks, and such virtual machines must be powered off before you take a snapshot. Snapshots of powered-on or suspended virtual machines with independent disks are not supported.

If you have **Independent** turned on in your virtual machines, the persistent attribute of the independent disk prevents a snapshot from being taken. To resolve this, power off the virtual machine, and disable the following options:

1. Go to **Inventory > Virtual Machine > Edit Settings**, and click the **Hardware** tab.
2. Under **Mode**, deselect **Independent**.

Resolving "VMDK is larger than the maximum size supported by datastore" Error

> This article refers to Barracuda Backup firmware version 5.0 or higher, and VMware ESX/ESXi 4.0 and higher with the VMware license which includes access to vSphere ® Data Recovery API.

Use the steps in this article to resolve the error "VMDK is larger than the maximum size supported by datastore" encountered when creating an ESX/ESXi virtual machine snapshot.

In this article:

- Step 1. Determine Maximum File Size
        - ESXi 5.0 and 5.1 with VMFS5
    - ESX/ESXi 4.1 and ESXi 5.1 with VMFS3
    - ESX/ESXi 4.0 with VMFS3
- Step 2. Move Files to Accommodate Space Requirements
- Step 3. Calculate Required Overhead

Barracuda Networks Technical Support

- VMware KB Solution: Creating a snapshot for a virtual machine fails with the error: File is larger than maximum file size supported (1012384)

In the vSphere Client, you may see the error:

```
File is larger than the maximum size supported by datastore.
```

In the hostd log file, you may see the error:

```
Snapshot guest failed: The file is too big for the filesystem.
```

In the vmware.log file of the virtual machine, you may see an error similar to:

```
vmx| FILE: File_VMFSSupportsFileSize: Requested file size ( 554051831808) larger than maximum
supported filesystem file size (274877906944)
vmx| DiskLibCreateCustom: if your disk is on VMFS, you may consider increasing the block size.
vmx| DISKLIB-LIB : Failed to create link: The destination file system does not support large files
(12)
vmx| SNAPSHOT: BranchDisk: Failed to create child disk ' /vmfs/volumes/uuid/vmname/vmname-000001.vmdk'
: The destination file system does not support large files (12)
vmx| SNAPSHOT: SnapshotBranch failed: The destination file system does not support large files (5).
vmx| [msg.checkpoint.save.fail2.std3] Error encountered while saving snapshot.
vmx| The destination file system does not support large files.
```

These errors occur when the snapshot file has exceeded the maximum size to fit in a datastore. Beginning with version 4.0, ESX/ESXi compares the maximum size of a snapshot redolog file to the maximum size of files on the datastore. The redolog file may not work correctly once it reaches the maximum size of the datastore. If the file can grow beyond the maximum size, ESX cancels the **Create Snapshot** operation and displays the `File is larger than the maximum size supported by datastore` error message.

ESX/ESXi 3.5 and Earlier
This does not apply to ESX/ESXi versions prior to 4.0; in prior versions, a snapshot is created even if there is insufficient space to store the full size redolog.

Use the following steps to resolve this error:

Step 1. Determine Maximum File Size

1. Compare the base disk size of the virtual machine against the block size of the datastore which contains the working directory of the virtual machine. By default, the working directory contains the virtual machine's **.vmx** configuration file. Note that the maximum file size differs among versions of ESX/ESXi and among versions of VMFS.
2. If you experience this error even after confirming that the snapshot files can fit on the datastore, proceed to **Step 3**.

A virtual machine on NFS or VMFS has a maximum virtual disk size of 2TB - 512Bytes, the same as the maximum in each of these tables.

ESXi 5.0 and 5.1 with VMFS5

On ESXi 5.0 and 5.1 and newly formatted VMFS5, a standard 1MB block size is available. The maximum file size is 2TB - 512Bytes.

- Block Size **1MB** / Maximum File Size **2TB - 512 Bytes**

> On ESXi 5 hosts using VMFS5 upgraded from VMFS3, upgraded volumes inherit the VMFS3 block size. The default block size for new volumes is 1MB. The maximum file size, regardless of block size, is 2TB - 512Bytes. For more information, see the *Storage Maximums* table in Configuration Maximums for VMware vSphere 5.0.

ESX/ESXi 4.1 and ESXi 5.1 with VMFS3

On ESX/ESXi 4.1 and ESXi 5.1 using a VMFS3 datastore, the maximum file size corresponds to the block size of the VMFS datastore:

- Block Size **1MB** / Maximum File Size **256GB**
- Block Size **2MB** / Maximum File Size **512GB**
- Block Size **4MB** / Maximum File Size **1TB**
- Block Size **8MB** / Maximum File Size **2TB - 512 Bytes**

ESX/ESXi 4.0 with VMFS3

On ESX/ESXi 4.0, the maximum file size corresponds to the block size of the VMFS3 datastore:

- Block Size **1MB** / Maximum File Size **256GB - 512Bytes**
- Block Size **2MB** / Maximum File Size **512GB - 512Bytes**
- Block Size **4MB** / Maximum File Size **1TB - 512Bytes**
- Block Size **8MB** / Maximum File Size **2TB - 512 Bytes**

Step 2. Move Files to Accommodate Space Requirements

This step describes how to resolve this error by changing either the location of the virtual machine configuration files or the workingDir to a datastore with enough block size.

The **workingDir** is the location where the snapshots are created, By default, the workingDir contains the virtual machine's **.vmx** configuration file. To change the workingDir directory to a datastore with enough block size, see the VMware solution Creating snapshots in a different location than default virtual machine directory (1002929).

To move the virtual machine's disks and/or configuration files, use Storage vMotion or cold migration with relocation of files. For more information, see the following VMware documentation:

- vSphere 5: *Migrating Virtual Machines* section of the vCenter Server and Host Management Guide.
- vSphere 4.1: *Migrating Virtual Machines* section of the vSphere Datacenter Administration Guide.
- vSphere 4.0: *Migrating Virtual Machines* section of the vSphere Basic System Administration Guide.

If the virtual machine already has snapshots, some procedures may not work, or they may attempt to create a snapshot. This table lists the requirements for the various procedures:

Procedure	Requirements
Storage vMotion	The virtual machine must not have snapshots on ESX/ESXi 4.1 hosts or earlier. It may have snapshots on ESXi 5.0 or later.
Cold migration with file relocation	The virtual machine may have snapshots. The source and destination hosts must be running ESX/ESXi 3.5 or later.
Change workingDir	The virtual machine may have snapshots. When new snapshots are created, new redologs are placed in the workingDir directory.

Hot clone	The virtual machine may have snapshots, but the snapshot hierarchy must be less than 31 snapshots deep. Hot cloning a virtual machine creates a snapshot on the source at the beginning of the process, and then deletes the snapshot at the end of the process.
Cold clone	The virtual machine may have snapshots. Cloning the virtual machine creates a new virtual machine with the same content as the original virtual machine, but without snapshots.
vMotion to ESX/ESXi 3.5	The virtual machine may have snapshots. The virtual machine must use hardware version 4. ESX/ESXi 3.5 does not perform the check described here and allows snapshots to be created.

Step 3. Calculate Required Overhead

The failure depends on the size of the virtual disk. All virtual machines that have disks greater than the maximum supported size by VMFS may experience this error. Overhead for the snapshot is approximately 2GB for a disk size of 256GB. If snapshots are to be used, consider the overhead while deciding the size of the disks:

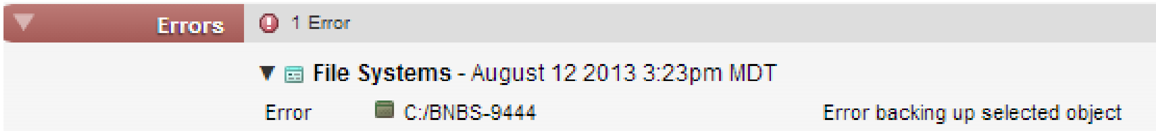
Maximum VMDK Size	Maximum Overhead	Maximum Size Less Overhead
256GB - 512B	~ 2GB	254GB
512GB - 512B	~ 4GB	508GB
1TB - 512B	~ 8GB	1TB
2TB - 512B	~ 16GB	2TB

VMware recommends that you create virtual disks that are smaller than the maximum size minus the overhead to enable the use of features such as snapshotting, cloning, and independent non-persistent disks.

Resolving "Error backing up selected object" Error

This article refers to Barracuda Backup firmware version 5.0 or higher.

Through the Barracuda Backup web interface you can select specific folders for back up within a parent directory. However, if a folder that has been selected for backup is moved or removed from the parent directory, the Barracuda Backup Server generates an error because the item selected for back up is no longer present:

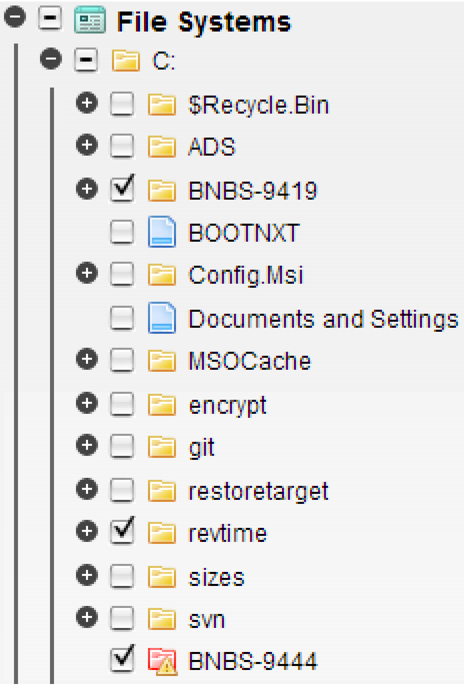


File Systems - August 12 2013 3:23pm MDT

Error C:/BNBS-9444 Error backing up selected object

To resolve this error, log in to the web interface and deselect the folder which has been removed from the directory for the source. To do so,

1. Log in to Barracuda Backup, and go to the **BACKUP > Sources** page.
2. Click **Edit** to the right of the source to edit share settings.
3. Expand the item selection. The folder displays with a warning triangle:



☐ File Systems
- ☐ C:
  - ☐ $Recycle.Bin
  - ☐ ADS
  - ☑ BNBS-9419
  - ☐ BOOTNXT
  - ☐ Config.Msi
  - ☐ Documents and Settings
  - ☐ MSOCache
  - ☐ encrypt
  - ☐ git
  - ☐ restoretarget
  - ☑ revtime
  - ☐ sizes
  - ☐ svn
  - ☑ BNBS-9444

4. Uncheck the removed folder, and click **Save** to save your settings.

> **Important**
> Deselecting folders and/or files purges the associated data from the Barracuda Backup Server.

Resolving "An unknown OS error occurred" Error

This article refers to Barracuda Backup firmware version 4.0 or higher.

This article describes how to resolve the error "Error occurred during backup initialization". If you encounter this error in the Backup Report on the Barracuda Backup Server, it may be caused by misconfigured or disabled Volume Shadow Copy Services (VSS) drivers. Microsoft provides a command-line tool to verify the state of the VSS writers. To utilize this tool, open a command prompt on the Windows Server, and enter: `vssadm in list writers`

Following is an example using this tool to check driver status:

```
C:\>vssadmin list writers

vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool (C) Copyright 2001
Microsoft Corp.

Writer name: 'System Writer'

Writer Id: {e8132975-6f93-4464-a53e-1050253ae220}

Writer Instance Id: {449e12cf-6b8f-4d75-a821-bc869d6612c4}

State: [1] Failed

Last error: No error



Writer name: 'SqlServerWriter'

Writer Id: {a65faa63-5ea8-4ebc-9dbd-a0c4db26912a}

Writer Instance Id: {de3b2861-77f6-43f8-8619-64dc9ea2fbcf}

State: [1] Stable
```

```
Last error: No error


Writer name: 'MSDEWriter'

Writer Id: {f8544ac1-0611-4fa5-b04b-f7ee00b03277}

Writer Instance Id: {9036fdfa-05ef-4f7d-9c2f-84fa2f06560a}

State: [1] Stable

Last error: No error


Writer name: 'WMI Writer'

Writer Id: {a6ad56c2-b509-4e6c-bb19-49d8f43532f0}

Writer Instance Id: {f9f92826-a3d4-486c-ade3-a4201deb8ad2}

State: [7] Failed

Last error: No error
```

If the output of this command contains writers with a state that is not **'Stable'**, you must restart the VSS service Volume Shadow Copy Services. If you continue to see this error in reports and agent logs even after restarting the services, register your VSS drivers use the following instructions:

- Windows Server 2003 and Windows Server 2003 R2 - Refer to the Microsoft Knowledgebase solution Error message when you run the "vssadmin list writers" command on a Windows Server 2003-based computer: "Error: 0x8000FFFF" for details.
- Windows Server 2008 and Windows Server 2008 R2 - VSS drivers on Windows Server 2008 and 2008 R2 can normally be reset by restarting the Services from the Management Console based on the Microsoft Knowledgebase solution No VSS writers are listed when you run vssadmin list writers on Windows Server 2008 .

  ⚠ **Important**
  Restarting VSS on Windows 2008 can cause unexpected behavior. Verify that *all* necessary writers (e.g., Hyper-V or Exchange) have restarted or data objects may not be detected or backed up. It is recommended that you reboot the Server in lieu of restarting the VSS writer components listed below, and verify that all appropriate Microsoft updates are installed.

If you determine that restarting Services is appropriate for your environment, complete the following steps:

1. Log in to the system, and click **Start**.
2. Enter **services.msc** in the Start Search box, and press **Enter**.
3. In the **Services** window, right-click each of the following services individually, and then click **Restart** :
   a. **COM+ Event System**
   b. **Volume Shadow Copy**
4. Close the **Services** window.
5. Open an elevated command prompt, enter `vssadmin list writers` , and then click **Enter** .
6. Verify that the VSS writers are listed.

ⓘ **Barracuda Networks Technical Support**
If you continue to experience problems with your VSS drivers in relation to your Barracuda Backup Server, contact Barracuda Networks Technical Support.

Error occurred during backup initialization

Resolve the "Failure while using USN journal" Error

This article refers to Barracuda Backup firmware version 5.0 and higher, the Barracuda Backup Agent (Windows), and Microsoft Windows Server 2003 and higher.

In this article:

- Deleting an Active USN Change Journal
- Adding a USN Change Journal

Related Articles

- Barracuda Backup Agent (Windows)

Additional Resources

- Change Journal Operations
- Fsutil usn

An Update Sequence Number (USN) Journal is a change journal of file and directory changes on the NTFS volume including a description of the change, and the name of the file or directory. Each log file is incremented for each entry in the journal. Log files are stored until they are deleted or storage runs out. If storage is exhausted, older log files are deleted and cannot be restored.

If too many file or directory changes are encountered on your Windows Server, you may encounter a max journal wrapping error causing slower Barracuda Backup Agent backups. While full backups should not be affected, you may encounter differential and incremental backup failure:

```
08/13/13 18:32:55 0x0001208 YUsnJournalManager: Info: USN journal backups have been disabled for volume:
C:\
08/13/13 18:43:09 0x0001208 YUsnJournalManager: Exception occurred while backing up volume changes:
Exception - Original: 12011 - 0x00002eeb Mapped:12011
Location:YUsnJournalManager::BackupVolumeChanges:D:\compile\source\ods++\server\vam\core\win\YUsnJournalMan
ager.cpp:214 Description:'Failure while using USN journal'
```

This article describes how to expand the maximum Update Sequence Number (USN) Journal size in Windows.

The following instructions apply only if the USN change Journal is available and readable.

Deleting an Active USN Change Journal

Use the following steps to remove the active USN change Journal using `fsutil usn deletejournal`.

fsutil usn Parameters

- `deletejournal` - Deletes the active USN change journal. Deleting the change journal impacts the File Replication Service (FRS) and the Indexing Service. Additionally, this negatively impacts FRS SYSVOL replication and replication between DFS link alternates during rescanning of the volume.
- `/D` - Disables the active USN change journal and returns I/O control while the change journal is being disabled.

1. Log in to your Windows Server, launch **cmd**, and run as *admin*.
2. Enter the following command:
   `fsutil usn queryjournal C:`
   Where "C" represents the backup or partition drive.
3. The USN change Journal settings display including its size in hex bytes. If the value is approximately 30MB, the backup can fail due to snapshot creation failure from lack of space.
4. Run the following command:
   `fsutil usn deletejournal /D C:`
5. The USN Journal is deleted and the size reset.
6. You can proceed with your backup.

Adding a USN Change Journal

Use the following steps to add a USN change Journal using `fsutil usn createjournal`.

1. Log in to your Windows Server, launch **cmd**, and run as *admin*.
2. Run the following command:
3. `fsutil usn createjournal m=2147483648 a=1 C:`
   Where "C" represents the backup or partition drive.
4. The USN Journal is added.

> Once the USN change Journal is recreated, Barracuda Backup goes through the entire file system which may result in a longer backup.

Slow Agent Backups

Monitoring Windows System Performance During Backup

> This article refers to Barracuda Backup firmware version 5.0 and higher, and Microsoft Windows 7, Windows 8, Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Vista, and Windows XP, except where noted.

During backup, your organization may encounter performance or resource contention. To reduce this possibility, first evaluate the systems in your environment for hardware-specific performance limitations. Once this is determined, configure data sources for backup, and then monitor system performance using a system performance monitoring tool.

Monitor Windows System Components

> This utility is available for Windows 7, Windows Server 2008 R2, Windows Server 2012, and Windows Vista.

Evaluate Windows system components using a tool such as Windows Performance Monitor to evaluate performance in real time during backup or by reviewing historical data. You can view the results in graph, histogram, or report form. This utility organizes the results by object, counter, and instance which you can customize as data collector sets:

- Performance counters
- Event trace data
- System configuration information (registry key values)

An object is a system resource category, and counters are the properties of that object. For example, **% Processor Time** and **Interrupts/sec** are counters for the **Processor** object.

For additional information, refer to the following Microsoft TechNet articles:

- Windows Performance Monitor
- Using Performance Monitor
- Creating Data Collector Sets

CPU Usage

If backups consume too much CPU processing, system performance is affected. To determine whether a system is consuming too much CPU processing during backup, monitor the **% Processor Time** counter for the **Processor** object. This counter measures the time the processor spends working on productive threads against time spent servicing requests. The normal range for the counter is 0-80%, with occasional spikes up to 100%. Consistent values over 80% indicate a potential performance hit on the CPU load.

To determine the number of processes waiting, monitor the **Process Queue Length** for the **System** object. A continuous value of two or more indicates too many threads are queued up for processing. If you encounter a sustained value of 0, verify that a non-zero value can display.

Determine the default scale for the **Process Queue Length** counter to determine the actual value. For example, if the scale is 10x, then a reading of 20 indicates 2 waiting processes.

Memory Usage

If memory usage is too high, backup operations are negatively affected. To determine the amount of committed virtual memory in bytes, use the **Committed Bytes** counter for the **Memory** object. Verify that the **Committed Bytes** value is not approaching the amount of physical memory. Additionally, determine hard page faults on the system. Hard page faults occur when requested information is not where the application expects it to be, and must be must be retrieved either from another location or from the page file. Review for both a sustained value, which may indicate memory usage is too high, as well as the number of hard page faults that represent the actual read/write requests. A high **Page Fault/sec** rate may negatively affect performance and indicate insufficient memory. To resolve hard page faults, use the **Page Faults/sec** counter on the **Memory** object.

Disk Load

Use the disk performance counters to evaluate disk subsystem performance including disk controller card, High disk load during backup negatively affects performance. I/O bus, and the disk. Use the **%Disk Time** counter on the **PhysicalDisk** object to determine the elapsed time that the disk processes read/write requests. Additionally, use the **Avg. Disk Queue Length** counter on the **PhysicalDisk** object to determine the number of processes waiting for the hard disk. A value greater than one that lasts for more than one second indicate multiple processes are waiting and indicate heavy disk load.

Enable Disk Performance Counters
If the disk performance counters are disabled, use the following steps to enable all disk performance counters:

1. At a command prompt, enter the following command:
   `diskperf -y`
2. Restart the Windows system. Once the system restarts, all disk performance counters are enabled.

For additional information on using `Diskperf`, refer to the Microsoft TechNet article Diskperf.

How to Increase Backup Performance

This article refers to Barracuda Backup firmware version 5.0 or higher.

It can take longer to back up multiple small files in comparison to one large file. To improve performance during backup, complete the following:

- Turn off virus scanning on Windows systems, this can double performance
- Upgrade network interface card (NIC) drivers to the latest release

Barracuda has encountered issues with several server network cards which were resolved by upgrading the network driver.

- Increase system background performance over foreground performance
  - Uninstall unused/unnecessary programs
  - Remove unnecessary files using a program such as Disk Cleanup to remove temporary files, empty the Recycle Bin, and to remove other unnecessary items
  - Run fewer programs when the Backup is scheduled to run
- Apply the latest service packs and system patches
- Review data fragmentation levels; you can set Disk Defragmenter to run on a schedule or run it manually
- If appropriate, add secondary physical disks to the system to increase performance
- Add additional memory to the system
- Use RAID devices for greater throughput
- Review the system controller
- Install the Barracuda Agent on a less used partition rather than a heavily used partition

For details on moving the Barracuda Backup Agent database to an alternate location, refer to the following articles:

- How to Manually Move the Barracuda Backup Agent (Windows) Database to an Alternate Location
- How to Manually Move the Barracuda Backup Agent (Linux) Database to an Alternate Location

Agents and Tools

Go to the **SYSTEM > Software Downloads** page in Barracuda Backup to download Tools and Backup Agents.

In this Section

Barracuda Backup Agent (Windows)

- How to Install and Use the Barracuda Backup Agent (Windows)
- How to Silently Install the Barracuda Backup Agent (Windows)
- Understanding the Barracuda Backup Agent (Windows) File Structure
- How to Manually Move the Barracuda Backup Agent (Windows) Database to an Alternate Location

Barracuda Backup Agent (Linux)

- How to Install and Use the Barracuda Backup Agent (Linux)
- How to Manually Move the Barracuda Backup Agent (Linux) Database to an Alternate Location

Related Troubleshooting and Error Message Articles

- How to Troubleshoot Using the Barracuda Backup Agent (Windows) Log File
- Understanding Why the Barracuda Backup Agent Moves to a New Volume
- How to Change the Barracuda Backup Agent Port Number
- How to Change the Barracuda Linux Backup Agent Port Number
- How to Create a Pre- or Post-Agent Backup Command Batch File or Script
- Resolving "Agent database moved to different location" Warning

Tools

- How to Edit Network Settings through the Barracuda Console
- Bare Metal Restore
- GroupWise Trusted Key Generation

Barracuda Backup Agent (Windows)

In this Section

- How to Install and Use the Barracuda Backup Agent (Windows)
- How to Silently Install the Barracuda Backup Agent (Windows)
- Understanding the Barracuda Backup Agent (Windows) File Structure
- How to Manually Move the Barracuda Backup Agent (Windows) Database to an Alternate Location

How to Install and Use the Barracuda Backup Agent (Windows)

This article refers to Barracuda Backup firmware version 5.2 and higher and Barracuda Backup Agent (Windows) 5.2 or higher.

In this article:

- Install Barracuda Backup Agent
- Add Data Sources
- Set Up Backup Schedules and Retention

Related Articles

- Barracuda Backup Agent File Structure
- Change Barracuda Backup Agent Port Number
- Command Prompt Install

Agent Software Requirements
Use the Barracuda Backup Agent (Windows) to back up your Microsoft® File System, Microsoft Exchange® Server, Microsoft SQL Server®, and system state.

Barracuda Backup Agent (Windows) 5.2 or higher supports the following Microsoft Windows systems:

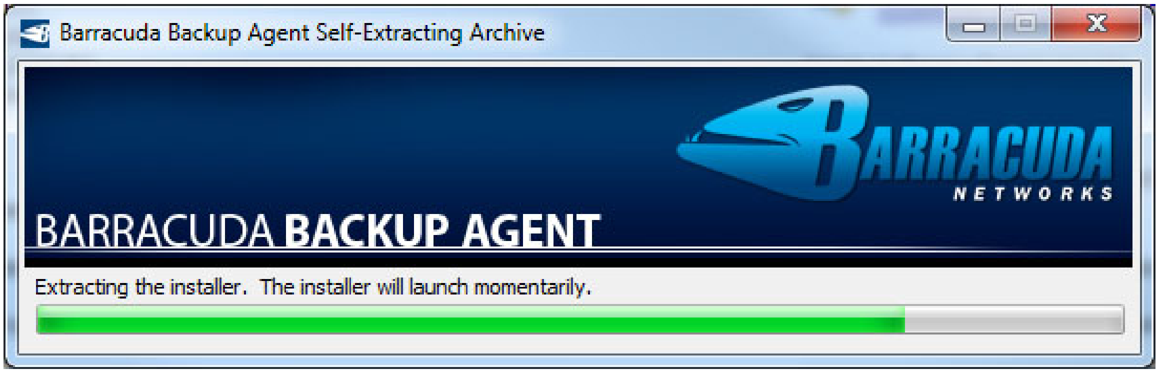
- Windows Server 2012
- Windows Server 2008
- Windows Server 2003 SP2 or higher
- Windows 7
- Windows Vista SP1 or higher
- Windows XP SP3 or higher (excluding System State)
- Windows 8

The Barracuda Agent is enabled by default for Windows Servers.

Install Barracuda Backup Agent

Use the following steps to install the Barracuda Backup Agent:

1. Log in to Barracuda Backup, and go to the **SYSTEM > Software Downloads** page.
2. Download the **Barracuda Backup Agent 5.2 (Windows)** to your local system or server.
3. Navigate to the download location, and run the executable; the installer self-extracts:



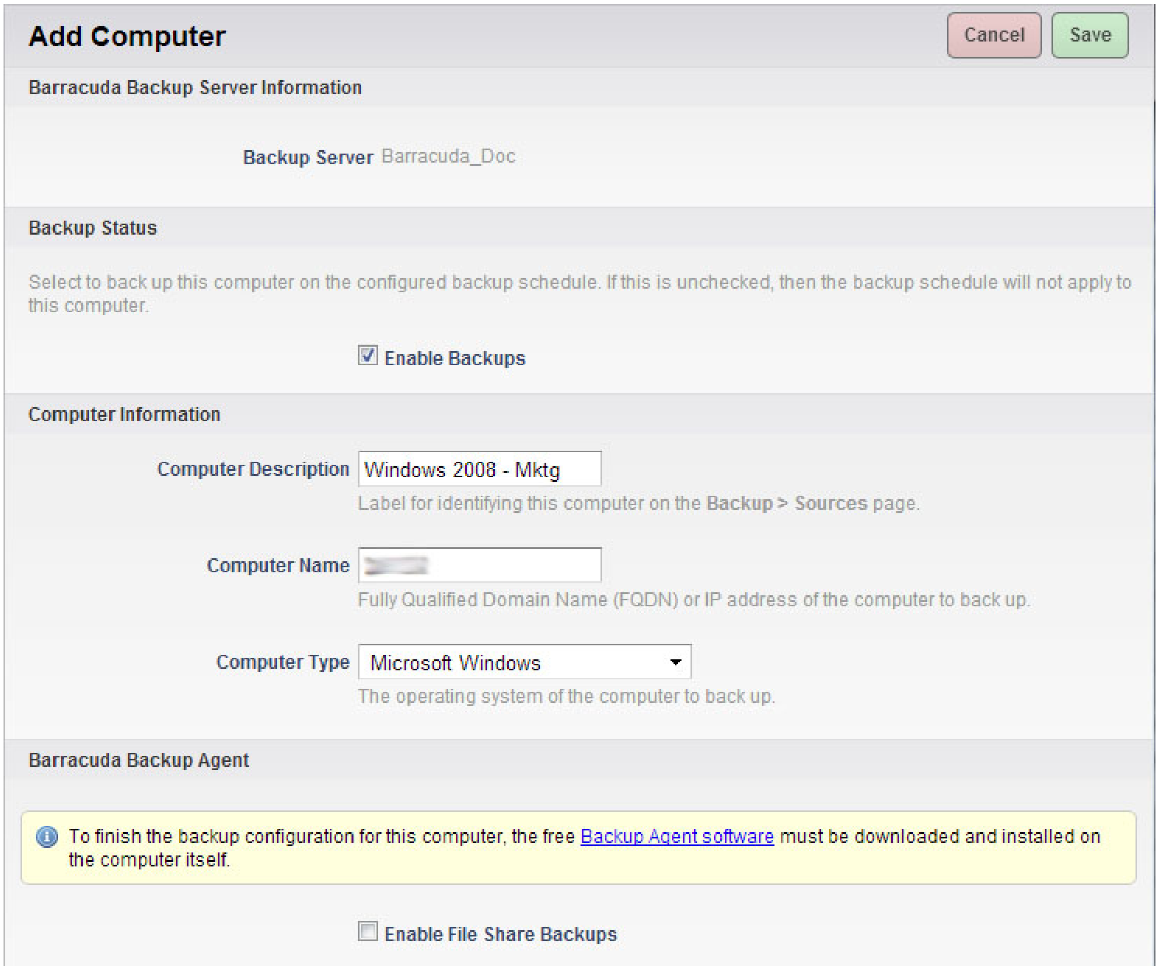
Extracting the installer. The installer will launch momentarily.

4. Follow the instructions in the wizard to complete the installation.

Add Data Sources

Use the following steps to add the Data Source to Barracuda Backup:

1. Log in to Barracuda Backup, and go to the **BACKUP > Sources** page.
2. Click **Add Computer**. Enter a computer description and enter the IP address or fully qualified domain name in the **Computer Name** field.
3. From the operating system drop-down menu, select Microsoft Windows:



Backup Server Barracuda_Doc

Select to back up this computer on the configured backup schedule. If this is unchecked, then the backup schedule will not apply to this computer.

☑ Enable Backups

Computer Description: Windows 2008 - Mktg

Label for identifying this computer on the **Backup > Sources** page.

Computer Name: [redacted]

Fully Qualified Domain Name (FQDN) or IP address of the computer to back up.

Computer Type: Microsoft Windows

The operating system of the computer to back up.

To finish the backup configuration for this computer, the free Backup Agent software must be downloaded and installed on the computer itself.

☐ Enable File Share Backups

4. Select whether to **Enable File Share Backups**.
5. Click **Save** at the top of the page. In the **Add Data Source** page, verify the **Data Type** displays as **Barracuda Agent Software**.
6. Click **Test Software Connectivity**; if the connection is successful, continue to the next step; however, if the connection is not successful, return to the **Add Computer** page and verify the IP address is correct before continuing. Click **Save** to return to the **Add Data Source** page.
7. If this is a SQL Server, complete the **Microsoft SQL Server Authentication** section.
8. In the **Item Selection** section, select the items you wish to back up.
9. Specify whether you wish to back up to cloud storage or replicate to another Barracuda Backup Server.
10. Click **Save** at the top of the page.

Set Up Backup Schedules and Retention

Once you have your data source items set up for backup, you can set up schedules and retention policies.

How to Silently Install the Barracuda Backup Agent (Windows)

This article refers to firmware version 5.2 and higher, and the Barracuda Backup Agent 5.0 and higher, and the Barracuda Backup Agent (Windows) 5.2 and higher.

Use the steps in this article to "silently" install the Barracuda Backup Agent on the server you wish to back up from a command prompt. These steps apply to either a new installation or an upgrade to a previously installed version of the Agent.

1. Log into the Barracuda Backup web interface, and go to the **SYSTEM > Software Downloads** page.
2. Under **Barracuda Backup Agent**, click **Download the latest version**, and download the **.exe** installer file to the system you intend to back up.
3. At a command prompt, change the directory to the location where you saved the Agent **.exe** installer file, and

enter the following command:

```
version number-win.exe -sp"-silent=Yes -upgrade=Yes"
```

Where *`version number`* represents the name of the downloaded **.exe** installer file. For example:

```
5.2.00-80572-win.exe -sp"-silent=Yes -upgrade=Yes"
```

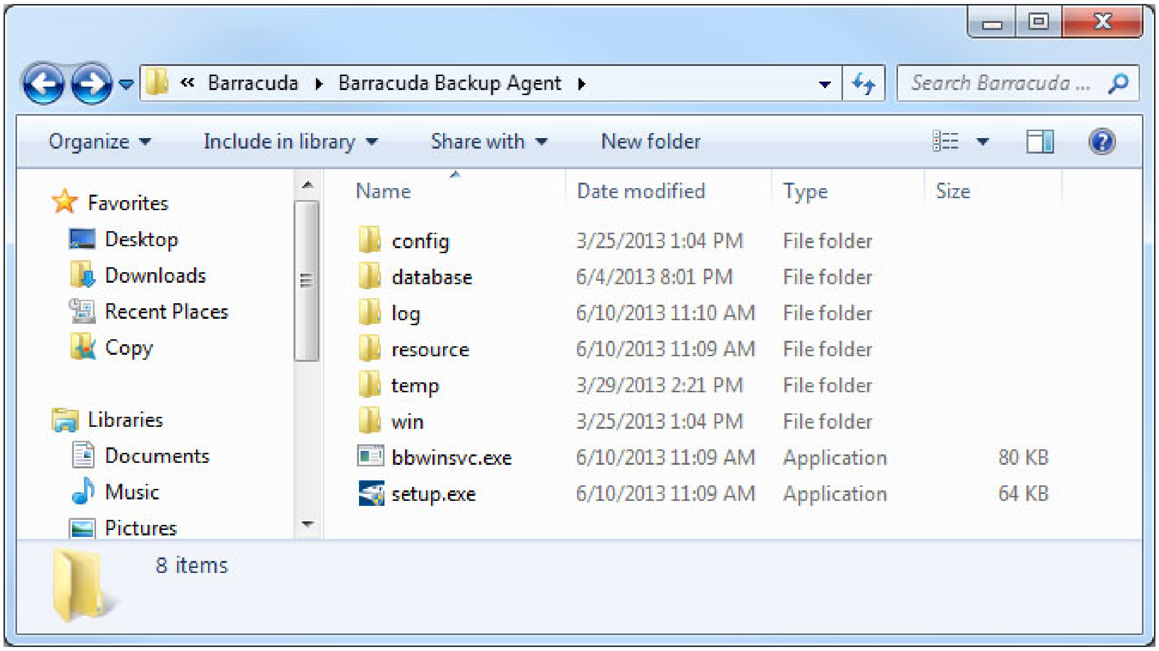
Understanding the Barracuda Backup Agent (Windows) File Structure

> This article refers to Barracuda Backup firmware version 5.0 and higher, and the Barracuda Backup Agent (Windows) version 5.0 and higher.

This article describes the overall file structure of the Barracuda Backup Agent (Windows) installation.

> ⚠ **Important**
> If the volume on which the Backup Agent is installed has less than 2GB available free space, the Backup Agent attempts to move its database to another volume. For details and resolution, see Understanding Why the Barracuda Backup Agent Moves to a New Volume.

The Barracuda Backup Agent default installation directory is: **C:\Program Files\Barracuda\Barracuda Backup Agent**


« Barracuda ▸ Barracuda Backup Agent ▸
Search Barracuda ...
Organize ▾
Include in library ▾
Share with ▾
New folder
Favorites
Desktop
Downloads
Recent Places
Copy
Libraries
Documents
Music
Pictures
8 items

Name	Date modified	Type	Size
config	3/25/2013 1:04 PM	File folder	
database	6/4/2013 8:01 PM	File folder	
log	6/10/2013 11:10 AM	File folder	
resource	6/10/2013 11:09 AM	File folder	
temp	3/29/2013 2:21 PM	File folder	
win	3/25/2013 1:04 PM	File folder	
bbwinsvc.exe	6/10/2013 11:09 AM	Application	80 KB
setup.exe	6/10/2013 11:09 AM	Application	64 KB

The following applications are contained in this directory:

File	Details
bbwinsvc.exe	Parent application that directs the appropriate **.exe** file located in the **win** folder.
setup.exe	Setup installation file.

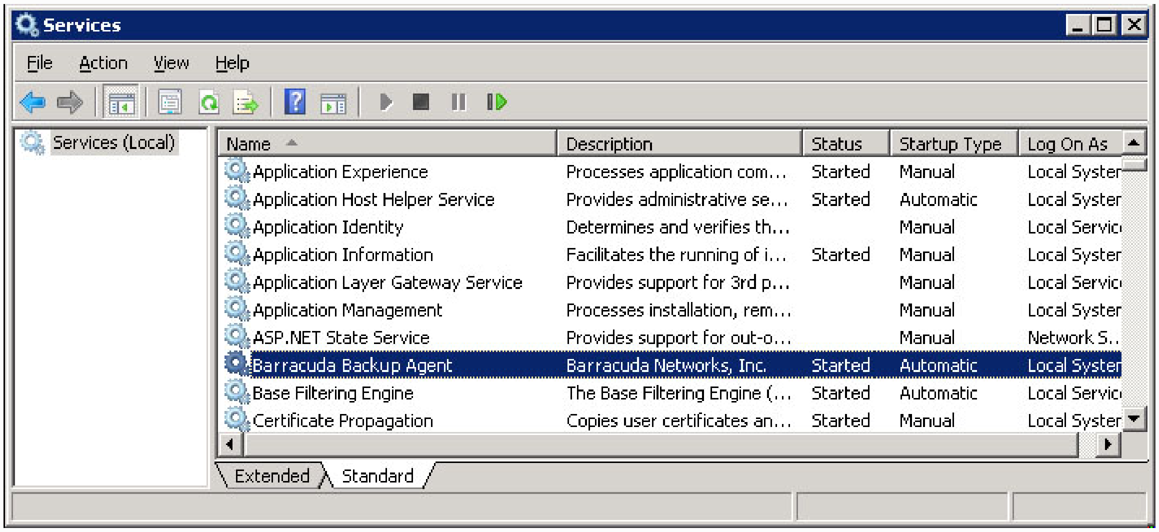
The following folders are contained within this directory:

Folder	Details

config	This folder contains the Barracuda Backup Agent configuration files including: - **bbconfig.ini** - Contains the Barracuda Backup Agent build number and installation version. Additionally, you can modify the file to take advantage of additional features, for example, change the Backup Agent port number, or leverage the Microsoft Volume Shadow Copy Service (VSS) to implement a full and differential SQL database backup operation. - **bbdetect.ini** - Initializes various Backup Agent features. If you do not want a feature to load, add a semicolon at the beginning of the line to comment it out. For example, you may want to comment out the SQL details. - **bbfilter.ini** - Initializes Backup Agent filters. - **bbinstall.ini** - Contains installation configuration settings.
database	Contains the local database used for source-based deduplication, and maintains the organization of the managed files for backup. This folder contains multiple **.dat** files.
log	Contains the Backup Agent log files; **bbtrtace.txt** is always the most recent log file. Each time the Backup Agent Service is restarted, a number is appended to the current **bbtrace.txt** file, and a new file is generated. Use these files to understand and resolve any errors that may occur with the Backup Agent such as an Agent backup initialization error.
resource	Contains the Backup Agent resource files.
temp	Remains empty unless an update is downloaded, at which time the update installer is temporarily added to this folder during installation.
win	Contains the **.dll** files and applications used by the Backup Agent Service.

Barracuda Backup Agent Service

The Backup Agent runs as a Service called Barracuda Backup Agent:



Name	Description	Status	Startup Type	Log On As
Application Experience	Processes application com...	Started	Manual	Local Syster
Application Host Helper Service	Provides administrative se...	Started	Automatic	Local Syster
Application Identity	Determines and verifies th...		Manual	Local Servic
Application Information	Facilitates the running of i...	Started	Manual	Local Syster
Application Layer Gateway Service	Provides support for 3rd p...		Manual	Local Servic
Application Management	Processes installation, rem...		Manual	Local Syster
ASP.NET State Service	Provides support for out-o...		Manual	Network S...
Barracuda Backup Agent	Barracuda Networks, Inc.	Started	Automatic	Local Syster
Base Filtering Engine	The Base Filtering Engine (...	Started	Automatic	Local Servic
Certificate Propagation	Copies user certificates an...	Started	Manual	Local Syster

Process Name

In the Task Manager, the process displays as **bbwinsdr**.

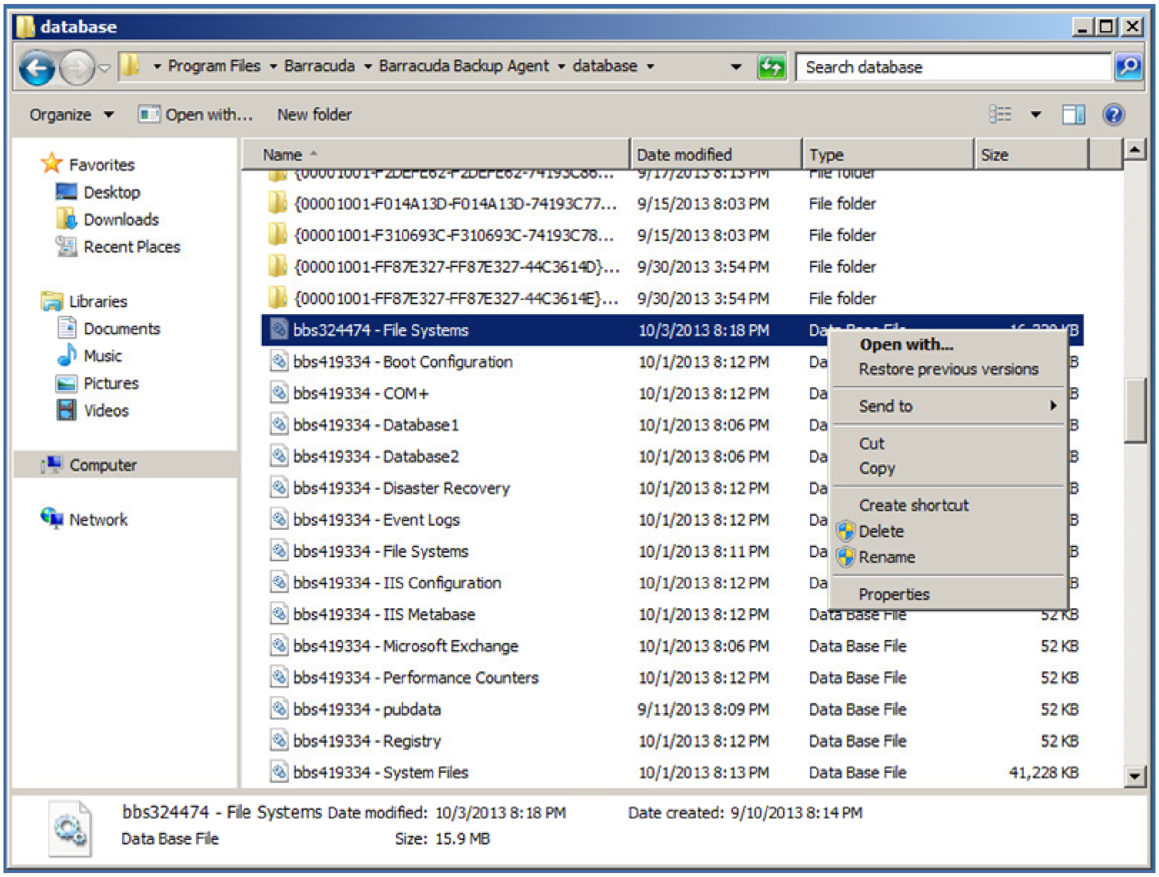
How to Manually Move the Barracuda Backup Agent (Windows) Database to an Alternate

Location

This article refers to firmware version 5.4 and higher, and the Barracuda Backup Agent (Windows).

In cases where the partition has limited space, use the following steps to move the Windows Backup Agent database.

1. Log in to the system where the Agent is installed.
2. Open the Agent database folder:
   C:\Program Files\Barracuda\Barracuda Backup Agent\database\
3. Copy the database named **bbs400000 - File Systems.db** and paste it into an alternate location.
4. Locate the Windows Agent configuration file **bbconfig.ini** in the default file location:
5. **C:\Program Files\Barracuda\Barracuda Backup Agent\config\bbconfig.ini**

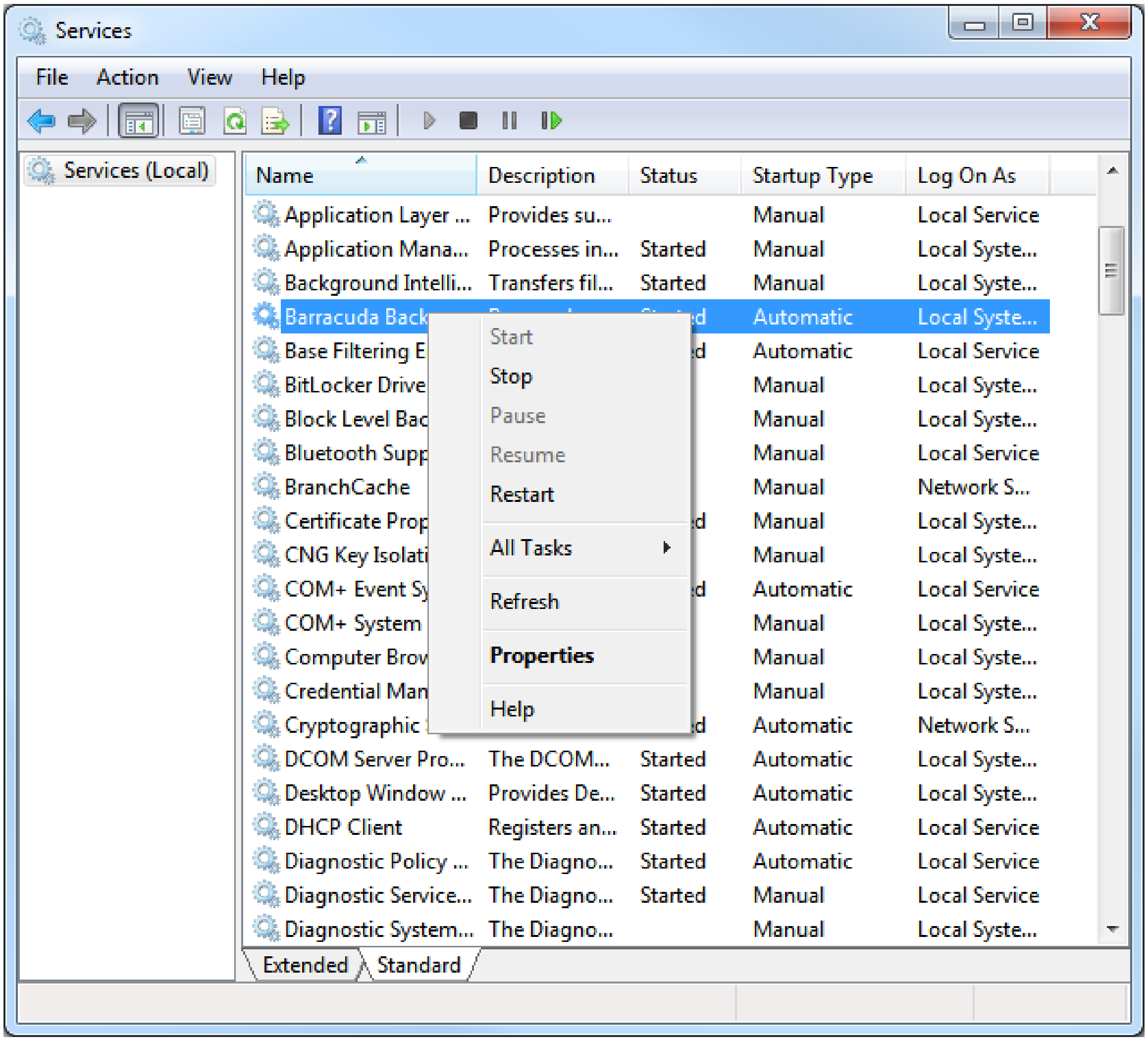

database
Program Files
Barracuda
Barracuda Backup Agent
database
Search database
Organize
Open with...
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Network
Open with...
Restore previous versions
Send to
Cut
Copy
Create shortcut
Delete
Rename
Properties

Name	Date modified	Type	Size
{00001001-F014A13D-F014A13D-74193C77...	9/15/2013 8:03 PM	File folder	
{00001001-F310693C-F310693C-74193C78...	9/15/2013 8:03 PM	File folder	
{00001001-FF87E327-FF87E327-44C3614D}...	9/30/2013 3:54 PM	File folder	
{00001001-FF87E327-FF87E327-44C3614E}...	9/30/2013 3:54 PM	File folder	
bbs324474 - File Systems	10/3/2013 8:18 PM	Da	KB
bbs419334 - Boot Configuration	10/1/2013 8:12 PM	Da	B
bbs419334 - COM+	10/1/2013 8:12 PM	Da	B
bbs419334 - Database1	10/1/2013 8:06 PM	Da	B
bbs419334 - Database2	10/1/2013 8:06 PM	Da	B
bbs419334 - Disaster Recovery	10/1/2013 8:12 PM	Da	B
bbs419334 - Event Logs	10/1/2013 8:12 PM	Da	B
bbs419334 - File Systems	10/1/2013 8:11 PM	Da	B
bbs419334 - IIS Configuration	10/1/2013 8:12 PM	Da	B
bbs419334 - IIS Metabase	10/1/2013 8:12 PM	Data Base File	52 KB
bbs419334 - Microsoft Exchange	10/1/2013 8:06 PM	Data Base File	52 KB
bbs419334 - Performance Counters	10/1/2013 8:12 PM	Data Base File	52 KB
bbs419334 - pubdata	9/11/2013 8:09 PM	Data Base File	52 KB
bbs419334 - Registry	10/1/2013 8:12 PM	Data Base File	52 KB
bbs419334 - System Files	10/1/2013 8:13 PM	Data Base File	41,228 KB

bbs324474 - File Systems Date modified: 10/3/2013 8:18 PM Date created: 9/10/2013 8:14 PM
Data Base File Size: 15.9 MB

6. Open **bbconfig.ini** using a text editor, and add the following lines to the end of the file:
   ```
   [fileStores]
   bbs400000 - File Systems=C:\Program Files\Barracuda\Barracuda Backup Agent\
   database\bbs400000 - File Systems.db
   ```
   Where *400000* represents the serial number of your Barracuda Backup Server.
   For example:
   ```
   [installControl]
   buildNumber=84642
   installedVersion=5.3.00-rel
   [configuration]
   nodeGuid={00001001-AC5CBCB7-AC4CBCB6-AC5CDCB8}
   [fileStores]
   bbs400000 - File Systems=C:\Program Files\Barracuda\Barracuda Backup
    Agent\database\bbs400000 - File Systems.db
   ```
7. Save and close the file.

8. Type `services.msc` in the **Start Search** box, and press **Enter**.
9. In the **Services** window, right-click **Barracuda Backup Agent**, and click **Restart**:



Name	Description	Status	Startup Type	Log On As
Application Layer ...	Provides su...		Manual	Local Service
Application Mana...	Processes in...	Started	Manual	Local Syste...
Background Intelli...	Transfers fil...	Started	Manual	Local Syste...
Barracuda Back		d	Automatic	Local Syste...
Base Filtering E		d	Automatic	Local Service
BitLocker Drive			Manual	Local Syste...
Block Level Bac			Manual	Local Syste...
Bluetooth Supp			Manual	Local Service
BranchCache			Manual	Network S...
Certificate Prop		d	Manual	Local Syste...
CNG Key Isolati			Manual	Local Syste...
COM+ Event Sy		d	Automatic	Local Service
COM+ System			Manual	Local Syste...
Computer Brov			Manual	Local Syste...
Credential Man			Manual	Local Syste...
Cryptographic		d	Automatic	Network S...
DCOM Server Pro...	The DCOM...	Started	Automatic	Local Syste...
Desktop Window ...	Provides De...	Started	Automatic	Local Syste...
DHCP Client	Registers an...	Started	Automatic	Local Service
Diagnostic Policy ...	The Diagno...	Started	Automatic	Local Service
Diagnostic Service...	The Diagno...	Started	Manual	Local Service
Diagnostic System...	The Diagno...		Manual	Local Syste...

Barracuda Backup Agent (Linux)

In this Section

- How to Install and Use the Barracuda Backup Agent (Linux)
- How to Manually Move the Barracuda Backup Agent (Linux) Database to an Alternate Location

How to Install and Use the Barracuda Backup Agent (Linux)

This article refers to Barracuda Backup firmware version 5.3 and higher, and the Barracuda Backup Agent (Linux).

In this article:

- Installing the Barracuda Backup Agent (Linux)
- Adding the Linux Data Source
- Backup Schedules and Retention

Agent Software Requirements
Barracuda Linux Backup Agent supports:

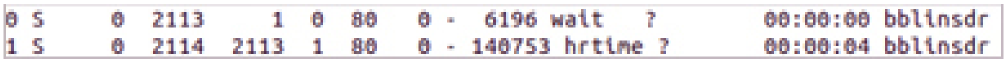
- Kernel 2.6.16 and higher
- glibc version 2.2.5 for 32-bit binary
- glibc version 2.3.4 for 64-bit binary

ⓘ **Backed Up Content**

Use the Barracuda Backup Agent (Linux) to back up Linux file systems such as Red Hat, Ubuntu, or SUSE. The Linux Agent can back up open files, permissions, soft and hard links, and supports multiple data streams.

Installing the Barracuda Backup Agent (Linux)

Use the following steps to install the Backup Agent:

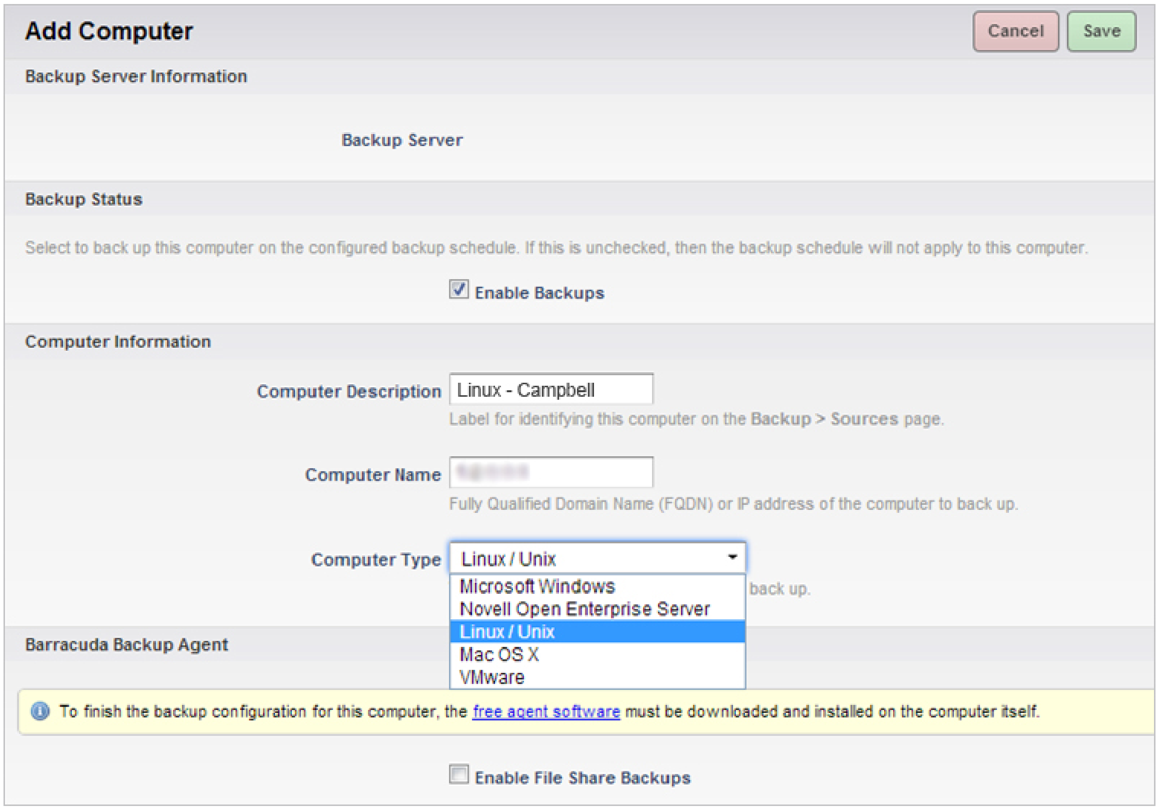
1. Log in to Barracuda Backup, and go to the **SYSTEM > Software Downloads** page.
2. Download and unzip the **Barracuda Backup Agent (Linux)** on your local Linux system or server.
3. Unpack the tar file:
   `tar -zxvf barracuda_backup_agent-x.x.x.tgz`
4. On your Linux system, open a terminal window, and change the directory to the Barracuda Linux Backup Agent directory, for example:
   `/Desktop/agent-5.3-lin$`
5. In the terminal window, run the command `sudo ./install`:
   Press **Enter** to install the Backup Agent in the default location:
   `[usr/local/barracuda/bbs]`
6. Once the Barracuda Linux Backup Agent installs, the Service automatically starts.
7. In the terminal window, run the command `ps-Al` to view the Barracuda Linux Backup Agent Service:
   

```
0 S     0  2113     1  0  80   0 -   6196 wait    ?        00:00:00 bblinsdr
1 S     0  2114  2113  1  80   0 - 140753 hrtime ?        00:00:04 bblinsdr
```

8. The Linux Backup Agent is now installed; close the terminal window.

Adding the Linux Data Source

Use the following steps to add the Linux Data Source to Barracuda Backup:

1. Log into Barracuda Backup, and go to the **BACKUP > Sources** page.
2. Click **Add Computer**. Enter a computer description and enter the IP address or fully qualified domain name in the **Computer Name** field.
3. From the operating system drop-down menu, select **Linux/Unix**:
   

Add Computer

Backup Server Information

Backup Server

Backup Status

Select to back up this computer on the configured backup schedule. If this is unchecked, then the backup schedule will not apply to this computer.

☑ Enable Backups

Computer Information

Computer Description: Linux - Campbell
Label for identifying this computer on the **Backup > Sources** page.

Computer Name: [redacted]
Fully Qualified Domain Name (FQDN) or IP address of the computer to back up.

Computer Type: Linux / Unix
back up.

Barracuda Backup Agent

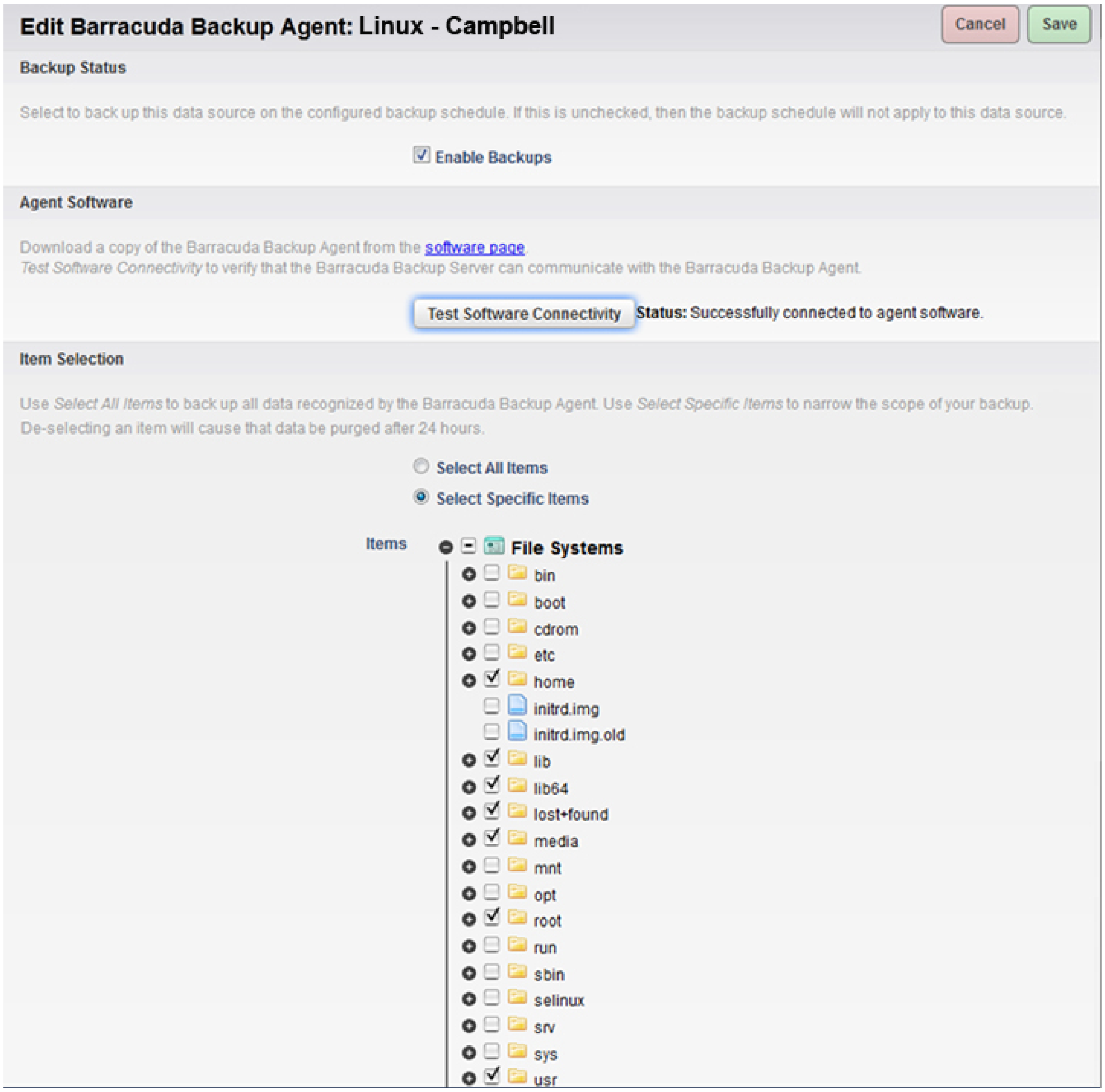
ⓘ To finish the backup configuration for this computer, the free agent software must be downloaded and installed on the computer itself.

☐ Enable File Share Backups

4. Click **Save** at the top of the page. In the **Edit** page, verify the **Data Type** displays as **Agent Software**.
5. Click **Test Software Connectivity**; if the connection is successful, continue to the next step; however, if the connection is not successful,

return to the **Add Computer** page and verify the IP address is correct before continuing. Click **Save** to return to the **Edit** page.

6. In the **Item Selection** section, select the items you wish to back up:



Edit Barracuda Backup Agent: Linux - Campbell

Backup Status

Select to back up this data source on the configured backup schedule. If this is unchecked, then the backup schedule will not apply to this data source.

☑ Enable Backups

Agent Software

Download a copy of the Barracuda Backup Agent from the software page.
Test Software Connectivity to verify that the Barracuda Backup Server can communicate with the Barracuda Backup Agent.

Status: Successfully connected to agent software.

Item Selection

Use *Select All Items* to back up all data recognized by the Barracuda Backup Agent. Use *Select Specific Items* to narrow the scope of your backup.
De-selecting an item will cause that data be purged after 24 hours.

○ Select All Items
● Select Specific Items

Items
- File Systems
  - ☐ bin
  - ☐ boot
  - ☐ cdrom
  - ☐ etc
  - ☑ home
  - ☐ initrd.img
  - ☐ initrd.img.old
  - ☑ lib
  - ☑ lib64
  - ☑ lost+found
  - ☑ media
  - ☐ mnt
  - ☐ opt
  - ☑ root
  - ☐ run
  - ☐ sbin
  - ☐ selinux
  - ☐ srv
  - ☐ sys
  - ☑ usr

7. Click **Save** at the top of the page.

Backup Schedules and Retention

Once you have your Linux data source items set up for backup, you can set up schedules and retention policies.

How to Manually Move the Barracuda Backup Agent (Linux) Database to an Alternate Location

This article refers to firmware version 5.3 and higher, and the Barracuda Backup Agent (Linux).

In cases where the partition has limited space, use the following steps to move the Backup Agent database.

1. At a command prompt, issue the following command where *40000* represents the serial number of your Barracuda Backup Server:

```
Mv /var/lib/bbs/database/bbs400000 - File Systems.db  /opt/database/bbs400000 -
File Systems.db
```

2. Locate the Linux Agent configuration file **bbconfig.ini** in the default file location:
/usr/local/barracuda/bbs/config/

3. Open **bbconfig.ini** using a text editor, and add the following lines to the end of the file:

```
[fileStores]

bbs400000 - File Systems=/mnt/harddrive2/Barracuda Backup Agent Database/bbs400000 - File Systems.db
```

Where `400000` represents the serial number of your Barracuda Backup Server.

4. Save the file.
5. Enter the following command to restart the Backup Agent:
   ```
   /etc/init.d/bbagent restart
   ```
6. View the **bbconfig.ini** file; it should look similar to:
   ```
   [installControl]

   buildNumber=84642

   installedVersion=5.3.00-rel



   [configuration]

   nodeGuid={00001001-AC5CBCB7-AC4CBCB6-AC5CDCB8}


   [fileStores]

   bbs438251 - File Systems=/opt/database/bbs400000 - File Systems.db
   ```
7. Close the **bbconfig.ini** file.

How to Edit Network Settings through the Barracuda Console

In this article:

- Console
- Interface
- Out-of-the-Box

Related Articles

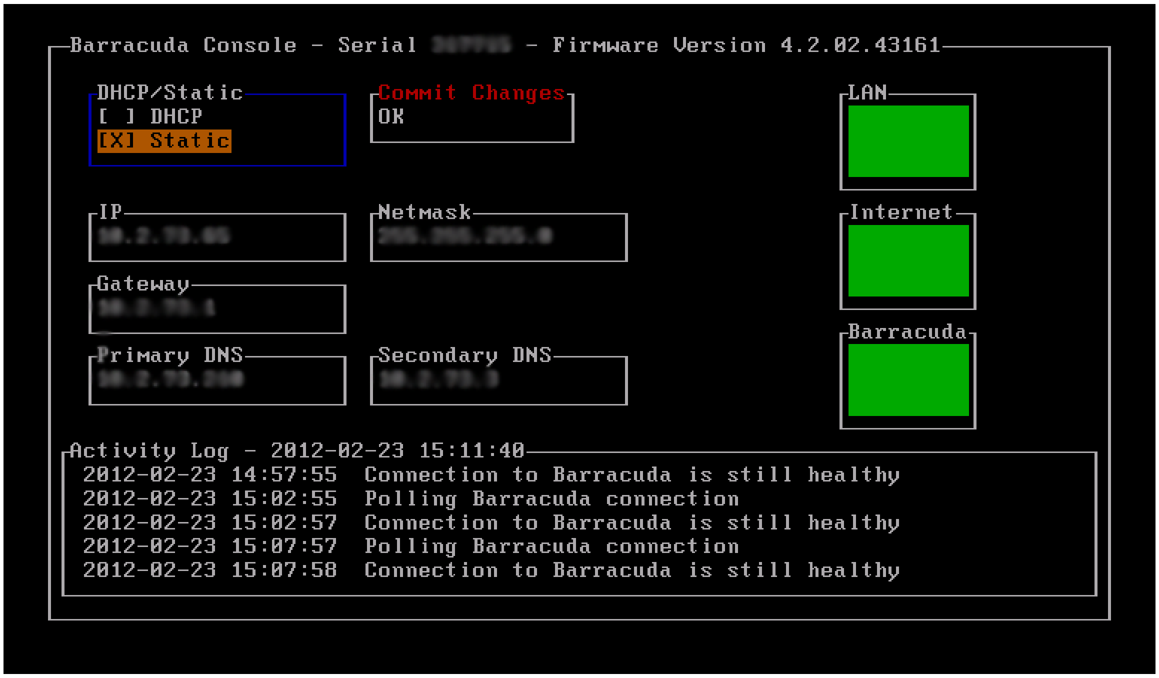
- Barracuda Backup Server Hardware Specifications
- Barracuda Backup Server Panel Indicators, Ports, and Connectors

Console

The Barracuda Console allows you to change the network settings on a Barracuda Backup Server directly. To access and interact with the Console screen, you must plug a keyboard and monitor into your Barracuda Backup Server.

Interface

The Console interface is a curses application that Barracuda Backup Servers boot into when started. Use the interface to change network settings through direct physical access to the unit:



```
Barracuda Console - Serial [redacted] - Firmware Version 4.2.02.43161

DHCP/Static          Commit Changes                 LAN
[ ] DHCP             OK                             🟩
[X] Static
                                                    Internet
IP                   Netmask                        🟩
[redacted]           [redacted]

Gateway                                             Barracuda
[redacted]                                          🟩

Primary DNS          Secondary DNS
[redacted]           [redacted]

Activity Log - 2012-02-23 15:11:40
 2012-02-23 14:57:55  Connection to Barracuda is still healthy
 2012-02-23 15:02:55  Polling Barracuda connection
 2012-02-23 15:02:57  Connection to Barracuda is still healthy
 2012-02-23 15:07:57  Polling Barracuda connection
 2012-02-23 15:07:58  Connection to Barracuda is still healthy
```

Out-of-the-Box

Making network setting changes using the Barracuda Console is easy. A Barracuda Backup Server is considered fully online when all three boxes, LAN, Internet, and Barracuda, are green. It is possible to have connectivity to the LAN and Internet but not to Barracuda Networks. This can occur if the system is not linked or if a LAN firewall is blocking the necessary outbound port 1194. Encrypted traffic is sent out across port 1194 to the Barracuda Networks management network.

If you wish to restrict the outbound network traffic on port 1194 to the Barracuda Networks specific IP range, please contact Barracuda Networks Technical Support for a listing of required IP addresses to allow. If a firewall is blocking outbound traffic on this port, the Barracuda Backup Server's Smartmode will be unable to bring the unit online.

If a DHCP server is running on the network, it is an easy way to bring the Barracuda Backup Server online. The Barracuda Backup Server requests network IP information from the DHCP server when it boots, or after it loses network connectivity for any reason. Static IP information can be specified on the Barracuda Backup Server as well.

Use the following keyboard commands to navigate and make changes in the Barracuda Console. The activity log shows you what the Barracuda Backup Server is doing during the process. Changes do not take effect until the **Commit Changes** button is highlighted and you press **Enter** on the keyboard:

- Arrow keys change field highlighting
- Spacebar selects DHCP or Static address
- Red headings are disabled fields due to the current mode
- Press **Enter** on **Commit Changes** when finished
- After changes are committed, the Barracuda Backup Server attempts to connect to Barracuda Networks

If you have questions about Barracuda Console, or need assistance getting your Barracuda Backup Server online, please contact Barracuda Networks Technical Support.

Hardware Compliance

This article contains appliance compliance information.

Notice for the USA

Compliance Information Statement (Declaration of Conformity Procedure) DoC FCC Part 15: This device complies with part 15 of the FCC Rules. Operation is subject to the following conditions:

This device may not cause harmful interference, and

This device must accept any interference received including interference that may cause undesired operation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user in encouraged to try one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Plug the equipment into an outlet on a circuit different from that of the receiver.
- Consult the dealer or an experienced radio/television technician for help.

Notice for Canada

This apparatus complies with the Class B limits for radio interference as specified in the Canadian Department of Communication Radio Interference Regulations.

Notice for Europe (CE Mark)

This product is in conformity with the Council Directive 89/336/EEC, 92/31/EEC (EMC).

Power Requirements

AC input voltage 100-240 volts; frequency 50/60 Hz.

Limited Warranty and License

Barracuda Networks Limited Hardware Warranty (v 2.1)

Barracuda Networks, Inc., or the Barracuda Networks, Inc. subsidiary or authorized Distributor selling the Barracuda Networks product, if sale is not directly by Barracuda Networks, Inc., ("Barracuda Networks") warrants that commencing from the date of delivery to Customer (but in case of resale by a Barracuda Networks reseller, commencing not more than sixty (60) days after original shipment by Barracuda Networks, Inc.), and continuing for a period of one (1) year: (a) its products (excluding any software) will be free from material defects in materials and workmanship under normal use; and (b) the software provided in connection with its products, including any software contained or embedded in such products will substantially conform to Barracuda Networks published specifications in effect as of the date of manufacture. Except for the foregoing, the software is provided as is. In no event does Barracuda Networks warrant that the software is error free or that Customer will be able to operate the software without problems or interruptions. In addition, due to the continual development of new techniques for intruding upon and attacking networks, Barracuda Networks does not warrant that the software or any equipment, system or network on which the software is used will be free of vulnerability to intrusion or attack. The limited warranty extends only to you the original buyer of the Barracuda Networks product and is non-transferable.

Exclusive Remedy

Your sole and exclusive remedy and the entire liability of Barracuda Networks under this limited warranty shall be, at Barracuda Networks or its service centers option and expense, the repair, replacement or refund of the purchase price of any products sold which do not comply with this warranty. Hardware replaced under the terms of this limited warranty may be refurbished or new equipment substituted at Barracuda Networks' option. Barracuda Networks obligations hereunder are conditioned upon the return of affected articles in accordance with Barracuda Networks then-current Return Material Authorization ("RMA") procedures. All parts will be new or refurbished, at Barracuda Networks' discretion, and shall be furnished on an exchange basis. All parts removed for replacement will become the property of Barracuda Networks. In connection with warranty services hereunder, Barracuda Networks may at its discretion modify the hardware of the product at no cost to you to improve its reliability or performance. The warranty period is not extended if Barracuda Networks repairs or replaces a warranted product or any parts. Barracuda Networks may change the availability of limited warranties, at its discretion, but any changes will not be retroactive. IN NO EVENT

SHALL BARRACUDA NETWORKS LIABILITY EXCEED THE PRICE PAID FOR THE PRODUCT FROM DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OF THE PRODUCT, ITS ACCOMPANYING SOFTWARE, OR ITS DOCUMENTATION.

Exclusions and Restrictions

This limited warranty does not apply to Barracuda Networks products that are or have been (a) marked or identified as "sample" or "beta," (b) loaned or provided to you at no cost, (c) sold "as is," (d) repaired, altered or modified except by Barracuda Networks, (e) not installed, operated or maintained in accordance with instructions supplied by Barracuda Networks, or (f) subjected to abnormal physical or electrical stress, misuse, negligence or to an accident.
EXCEPT FOR THE ABOVE WARRANTY, BARRACUDA NETWORKS MAKES NO OTHER WARRANTY, EXPRESS, IMPLIED OR STATUTORY, WITH RESPECT TO BARRACUDA NETWORKS PRODUCTS, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTY OF TITLE, AVAILABILITY, RELIABILITY, USEFULNESS, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, OR ARISING FROM COURSE OF PERFORMANCE, DEALING, USAGE OR TRADE. EXCEPT FOR THE ABOVE WARRANTY, BARRACUDA NETWORKS' PRODUCTS AND THE SOFTWARE ARE PROVIDED "AS-IS" AND BARRACUDA NETWORKS DOES NOT WARRANT THAT ITS PRODUCTS WILL MEET YOUR REQUIREMENTS OR BE UNINTERRUPTED, TIMELY, AVAILABLE, SECURE OR ERROR FREE, OR THAT ANY ERRORS IN ITS PRODUCTS OR THE SOFTWARE WILL BE CORRECTED. FURTHERMORE, BARRACUDA NETWORKS DOES NOT WARRANT THAT BARRACUDA NETWORKS PRODUCTS, THE SOFTWARE OR ANY EQUIPMENT, SYSTEM OR NETWORK ON WHICH BARRACUDA NETWORKS PRODUCTS WILL BE USED WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK.

Barracuda Networks Software License Agreement (v 2.1)

PLEASE READ THIS SOFTWARE LICENSE AGREEMENT ("AGREEMENT") CAREFULLY BEFORE USING THE BARRACUDA NETWORKS SOFTWARE. BY USING THE BARRACUDA SOFTWARE YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS LICENSE. IF YOU ARE A CORPORATION, PARTNERSHIP OR SIMILAR ENTITY, THEN THE SOFTWARE LICENSE GRANTED UNDER THIS AGREEMENT IS EXPRESSLY CONDITIONED UPON ACCEPTANCE BY A PERSON WHO IS AUTHORIZED TO SIGN FOR AND BIND THE ENTITY. IF YOU ARE NOT AUTHORIZED TO SIGN FOR AND BIND THE ENTITY OR DO NOT AGREE WITH ALL THE TERMS OF THIS AGREEMENT, DO NOT USE THE SOFTWARE. IF YOU DO NOT AGREE TO THE TERMS OF THIS LICENSE YOU MAY RETURN THE SOFTWARE OR HARDWARE CONTAINING THE SOFTWARE FOR A FULL REFUND TO YOUR PLACE OF PURCHASE.

1. The software and documentation, whether on disk, in flash memory, in read only memory, or on any other media or in any other form (collectively "Barracuda Software") is licensed, not sold, to you by Barracuda Networks, Inc. ("Barracuda") for use only under the terms of this Agreement, and Barracuda reserves all rights not expressly granted to you. The rights granted are limited to Barracuda's intellectual property rights in the Barracuda Software and do not include any other patent or intellectual property rights. You own the media on which the Software is recorded but Barracuda retains ownership of the Software itself. If you have not completed a purchase of the Software and made payment for the purchase, the Software may only be used for evaluation purposes and may not be used in any production capacity. Furthermore the Software, when used for evaluation, may not be secure and may use publicly available passwords.

2. Permitted License Uses and Restrictions. If you have purchased a Barracuda Networks hardware product, this Agreement allows you to use the Software only on the single Barracuda labeled hardware device on which the software was delivered. You may not make copies of the Software. You may not make a backup copy of the Software. If you have purchased a Barracuda Networks Virtual Machine you may use the software only in the licensed number of instances of the licensed sizes and you may not exceed the licensed capacities. You may make a reasonable number of backup copies of the Software. If you have purchased client software you may install the software only on the number of licensed clients. You may make a reasonable number of backup copies of the Software. For all purchases you may not modify or create derivative works of the Software except as provided by the Open Source Licenses included below. You may not make the Software available over a network where it could be utilized by multiple devices or copied. Unless otherwise expressly provided in the documentation, your use of the Software shall be limited to use on a single hardware chassis, on a single central processing unit, as applicable, or use on such greater number of chassis or central processing units as you may have paid Barracuda Networks the required license fee; and your use of the Software shall also be limited, as applicable and set forth in your purchase order or in Barracuda Networks' product catalog, user documentation, or web site, to a maximum number of (a) seats (i.e. users with access to install Software), (b) concurrent users, sessions, ports, and/or issued and outstanding IP addresses, and/or (c) central processing unit cycles or instructions per second. Your use of the Software shall also be limited by any other restrictions set forth in your purchase order or in Barracuda Networks' product catalog, user documentation or web site for the Software. The BARRACUDA SOFTWARE IS NOT INTENDED FOR USE IN THE OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION OR COMMUNICATION SYSTEMS, LIFE SUPPORT MACHINES, OR OTHER EQUIPMENT IN WHICH FAILURE COULD LEAD TO DEATH, PERSONAL INJURY, OR ENVIRONMENTAL DAMAGE. YOU EXPRESSLY AGREE NOT TO USE IT IN ANY OF THESE OPERATIONS.

3. You may not transfer, rent, lease, lend, or sublicense the Software or allow a third party to do so. YOU MAY NOT OTHERWISE TRANSFER THE SOFTWARE OR ANY OF YOUR RIGHTS AND OBLIGATIONS UNDER THIS AGREEMENT. You agree that you will have no right and will not, nor will it assist others to: (i) make unauthorized copies of all or any portion of the Software; (ii) sell, sublicense, distribute, rent or lease the Software; (iii) use the Software on a service bureau, time sharing basis or other remote access system whereby third parties other than you can use or benefit from the use of the Software; (iv) disassemble, reverse engineer, modify, translate, alter, decompile or otherwise attempt to discern

the source code of all or any portion of the Software; (v) utilize or run the Software on more computers than you have purchased license to; (vi) operate the Software in a fashion that exceeds the capacity or capabilities that were purchased by you.

4. THIS AGREEMENT SHALL BE EFFECTIVE UPON INSTALLATION OF THE SOFTWARE OR PRODUCT AND SHALL TERMINATE UPON THE EARLIER OF: (A) YOUR FAILURE TO COMPLY WITH ANY TERM OF THIS AGREEMENT OR (B) RETURN, DESTRUCTION OR DELETION OF ALL COPIES OF THE SOFTWARE IN YOUR POSSESSION. Rights of Barracuda Networks and your obligations shall survive any termination of this Agreement. Upon termination of this Agreement by Barracuda Networks, You shall certify in writing to Barracuda Networks that all copies of the Software have been destroyed or deleted from any of your computer libraries, storage devices, or any other location.

5. YOU EXPRESSLY ACKNOWLEDGE AND AGREE THAT THE USE OF THE BARRACUDA SOFTWARE IS AT YOUR OWN RISK AND THAT THE ENTIRE RISK AS TO SATISFACTION, QUALITY, PERFORMANCE, AND ACCURACY IS WITH YOU. THE BARRACUDA SOFTWARE IS PROVIDED "AS IS" WITH ALL FAULTS AND WITHOUT WARRANTY OF ANY KIND, AND BARRACUDA HEREBY DISCLAIMS ALL WARRANTIES AND CONDITIONS WITH RESPECT TO THE BARRACUDA SOFTWARE, EITHER EXPRESSED OR IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES AND/OR CONDITIONS OF MERCHANTIBILITY, OF SATISFACTORY QUALITY, OF FITNESS FOR ANY APPLICATION, OF ACCURACY, AND OF NON-INFRINGEMENT OF THIRD PARTY RIGHTS. BARRACUDA DOES NOT WARRANT THE CONTINUED OPERATION OF THE SOFTWARE, THAT THE PERFORMANCE WILL MEET YOUR EXPECTATIONS, THAT THE FUNCTIONS WILL MEET YOUR REQUIREMENTS, THAT THE OPERATION WILL BE ERROR FREE OR CONTINUOUS, THAT CURRENT OR FUTURE VERSIONS OF ANY OPERATING SYSTEM WILL BE SUPPORTED, OR THAT DEFECTS WILL BE CORRECTED. NO ORAL OR WRITTEN INFORMATION GIVEN BY BARRACUDA OR AUTHORIZED BARRACUDA REPRESENTATIVE SHALL CREATE A WARRANTY. SHOULD THE BARRACUDA SOFTWARE PROVE DEFECTIVE, YOU ASSUME THE ENTIRE COST OF ALL NECESSARY SERVICING, REPAIR, OR CORRECTION. FURTHERMORE BARRACUDA NETWORKS SHALL ASSUME NO WARRANTY FOR ERRORS/BUGS, FAILURES OR DAMAGE WHICH WERE CAUSED BY IMPROPER OPERATION, USE OF UNSUITABLE RESOURCES, ABNORMAL OPERATING CONDITIONS (IN PARTICULAR DEVIATIONS FROM THE INSTALLATION CONDITIONS) AS WELL AS BY TRANSPORTATION DAMAGE. IN ADDITION, DUE TO THE CONTINUAL DEVELOPMENT OF NEW TECHNIQUES FOR INTRUDING UPON AND ATTACKING NETWORKS, BARRACUDA NETWORKS DOES NOT WARRANT THAT THE SOFTWARE OR ANY EQUIPMENT, SYSTEM OR NETWORK ON WHICH THE SOFTWARE IS USED WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK. YOU EXPRESSLY ACKNOWLEDGE AND AGREE THAT YOU WILL PROVIDE AN UNLIMITED PERPETUAL ZERO COST LICENSE TO BARRACUDA FOR ANY PATENTS OR OTHER INTELLECTUAL PROPERTY RIGHTS WHICH YOU EITHER OWN OR CONTROL THAT ARE UTILIZED IN ANY BARRACUDA PRODUCT.

6. Termination and Fair Use Policy. BARRACUDA SHALL HAVE THE ABSOLUTE AND UNILATERAL RIGHT AT ITS SOLE DISCRETION TO DENY USE OF, OR ACCESS TO BARRACUDA SOFTWARE, IF YOU ARE DEEMED BY BARRACUDA TO BE USING THE SOFTWARE IN A MANNER NOT REASONABLY INTENDED BY BARRACUDA OR IN VIOLATION OF ANY LAW.

7. Limitation of Liability. TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT SHALL BARRACUDA BE LIABLE FOR PERSONAL INJURY OR ANY INCIDENTAL SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, LOSS OF DATA, BUSINESS INTERRUPTION, OR ANY OTHER COMMERCIAL DAMAGES OR LOSSES, ARISING OUT OF OR RELATED TO YOUR ABILITY TO USE OR INABILITY TO USE THE BARRACUDA SOFTWARE HOWEVER CAUSED, REGARDLESS OF THE THEORY OF LIABILITY AND EVEN IF BARRACUDA HAS BEEN ADVISED OF THE POSSIBILITY OF DAMAGES. In no event shall Barracuda's total liability to you for all damages exceed the amount of one hundred dollars.The following terms govern your use of the Energize Update Software except to the extent a particular program (a) is the subject of a separate written agreement with Barracuda Networks or (b) includes a separate "click-on" license agreement as part of the installation and/or download process. To the extent of a conflict between the provisions of the foregoing documents, the order of precedence shall be (1) the written agreement, (2) the click-on agreement, and (3) this Energize Update Software License.

8. Content Restrictions. YOU MAY NOT (AND MAY NOT ALLOW A THIRD PARTY TO) COPY, REPRODUCE, CAPTURE, STORE, RETRANSMIT, DISTRIBUTE, OR BURN TO CD (OR ANY OTHER MEDIUM) ANY COPYRIGHTED CONTENT THAT YOU ACCESS OR RECEIVE THROUGH USE OF THE PRODUCT CONTAINING THE SOFTWARE. YOU ASSUME ALL RISK AND LIABILITY FOR ANY SUCH PROHIBITED USE OF COPYRIGHTED CONTENT. You agree not to publish any benchmarks, measurements, or reports on the product without Barracuda Networks’ written express approval.

9. Third Party Software. Some Software which supports Bare Metal Disaster Recovery of Microsoft Windows Vista and Microsoft Windows 2008 Operating Systems (DR6) contains and uses components of the Microsoft Windows Pre-Installation Environment (WINPE) with the following restrictions: (i) the WINPE components in the DR6 product are licensed and not sold and may only be used with the DR6 product; (ii) DR6 is provided "as is"; (iii) Barracuda and its suppliers reserve all rights not expressly granted; (iv) license to use DR6 and the WINPE components is limited to use of the product as a recovery utility program only and not for use as a general purpose operating system; (v) Reverse engineering, decompiling or disassembly of the WINPE components, except to the extent expressly permitted by applicable law, is prohibited; (vi) DR6 contains a security feature from Microsoft that will automatically reboot the system without warning after 24 hours of continuous use; (vii) Barracuda alone will provide support for customer issues with DR6 and Microsoft and its Affiliates are released of all liability related to its use and operation; and, (viii) DR6 is subject to U.S. export jurisdiction.

10. Trademarks. Certain portions of the product and names used in this Agreement, the Software and the documentation may constitute trademarks of Barracuda Networks. You are not authorized to use any such trademarks for any purpose.

11. Export Restrictions. You may not export or re-export the Software without: (a) the prior written consent of Barracuda Networks, (b) complying with applicable export control laws, including, but not limited to, restrictions and regulations of the Department of Commerce or other United States agency or authority and the applicable EU directives, and (c) obtaining any necessary permits and licenses. In any event, you may not transfer or authorize the transfer of the Software to a prohibited territory or country or otherwise in violation of any applicable restrictions or regulations. If you are a United States Government agency the Software and documentation qualify as "commercial items", as that term is defined at Federal Acquisition Regulation ("FAR") (48 C.F.R.) 2.101, consisting of "commercial computer software" and "commercial computer software documentation" as such terms are used in FAR 12.212. Consistent with FAR 12.212 and DoD FAR Supp. 227.7202-1 through 227.7202-4, and notwithstanding any other FAR or other contractual clause to the contrary in any agreement into which this Agreement may be incorporated, Government end user will acquire the Software and documentation with only those rights set forth in this Agreement. Use of either the Software or documentation or both constitutes agreement by the Government that the Software and documentation are "commercial computer software" and "commercial computer software documentation", and constitutes acceptance of the rights and restrictions herein.

12. General. THIS AGREEMENT IS GOVERNED BY THE LAWS OF THE STATE OF CALIFORNIA, USA WITH JURISDICTION OF SANTA CLARA COUNTY, CALIFORNIA, UNLESS YOUR HEADQUARTERS IS LOCATED IN SWITZERLAND, THE EU, OR JAPAN. IF YOUR HEADQUARTERS IS LOCATED IN SWITZERLAND THE SWISS MATERIAL LAW SHALL BE USED AND THE JURISDICTION SHALL BE ZURICH. IF YOUR HEADQUARTERS IS LOCATED IN THE EU, AUSTRIAN LAW SHALL BE USED AND JURISDICTION SHALL BE INNSBRUCK. IF YOUR HEADQUARTERS IS LOCATED IN JAPAN, JAPANESE LAW SHALL BE USED AND JURISDICTION SHALL BE TOKYO. THIS AGREEMENT WILL NOT BE SUBJECT TO ANY CONFLICT-OF-LAWS PRINCIPLES IN ANY JURISDICTION. THIS AGREEMENT WILL NOT BE GOVERNED BY THE U.N. CONVENTION ON CONTRACTS FOR THE INTERNATIONAL SALES OF GOODS. This Agreement is the entire agreement between You and Barracuda Networks regarding the subject matter herein and supersedes any other communications with respect to the Software. If any provision of this Agreement is held invalid or unenforceable, the remainder of this Agreement will continue in full force and effect. Failure to prosecute a party's rights with respect to a default hereunder will not constitute a waiver of the right to enforce rights with respect to the same or any other breach.

13. Assignability. You may not assign any rights or obligations hereunder without prior written consent from Barracuda Networks.

14. Billing Issues. You must notify Barracuda of any billing problems or discrepancies within sixty (60) days after they first appear on the statement you receive from your bank, Credit Card Company, other billing company or Barracuda Networks. If you do not bring such problems or discrepancies to Barracuda Networks attention within the sixty (60) day period, you agree that you waive the right to dispute such problems or discrepancies.

15. Collection of Data. You agree to allow Barracuda Networks to collect information ("Statistics") from the Software in order to fight spam, virus, and other threats as well as optimize and monitor the Software. Information will be collected electronically and automatically. Statistics include, but are not limited to, the number of messages processed, the number of messages that are categorized as spam, the number of virus and types, IP addresses of the largest spam senders, the number of emails classified for Bayesian analysis, capacity and usage, and other statistics. Your data will be kept private and will only be reported in aggregate by Barracuda Networks.

16. Subscriptions. Software updates and subscription information provided by Barracuda Energize Updates or other services may be necessary for the continued operation of the Software. You acknowledge that such a subscription may be necessary. Furthermore some functionality may only be available with additional subscription purchases. Obtaining Software updates on systems where no valid subscription has been purchased or obtaining functionality where subscription has not been purchased is strictly forbidden and in violation of this Agreement. All initial subscriptions commence at the time of activation and all renewals commence at the expiration of the previous valid subscription. Unless otherwise expressly provided in the documentation, you shall use the Energize Updates Service and other subscriptions solely as embedded in, for execution on, or (where the applicable documentation permits installation on non-Barracuda Networks equipment) for communication with Barracuda Networks equipment owned or leased by you. All subscriptions are non-transferrable. Barracuda Networks makes no warranty that subscriptions will continue un-interrupted. Subscription may be terminated without notice by Barracuda Networks for lack of full payment.

17. Auto Renewals. If your Software purchase is a time based license, includes software maintenance, or includes a subscription, you hereby agree to automatically renew this purchase when it expires unless you notify Barracuda 15 days before the renewal date. Barracuda Networks will automatically bill you or charge you unless notified 15 days before the renewal date.

18. Time Base License. If your Software purchase is a time based license you expressly acknowledge that the Software will stop functioning at the time the license expires. You expressly indemnify and hold harmless Barracuda Networks for any and all damages that may occur because of this.

19. Support. Telephone, email and other forms of support will be provided to you if you have purchased a product that includes support. The hours of support vary based on country and the type of support purchased. Barracuda Networks Energize Updates typically include Basic support.

20. Changes. Barracuda Networks reserves the right at any time not to release or to discontinue release of any Software or Subscription and to alter prices, features, specifications, capabilities, functions, licensing terms, release dates, general availability or other characteristics of any future releases of the Software or Subscriptions.

21. Open Source Licensing. Barracuda Networks products may include programs that are covered by the GNU General Public License (GPL) or other Open Source license agreements, in particular the Linux operating system. It is expressly put on record that the Software does not

constitute an edited version or further development of the operating system. These programs are copyrighted by their authors or other parties, and the authors and copyright holders disclaim any warranty for such programs. Other programs are copyright by Barracuda Networks. Further details may be provided in an appendix to this agreement where the licenses are re-printed. Barracuda Networks makes available the source code used to build Barracuda products available at source.barracuda.com. This directory includes all the programs that are distributed on the Barracuda products. Obviously not all of these programs are utilized, but since they are distributed on the Barracuda product we are required to make the source code available.

Barracuda Networks Energize Updates and Other Subscription Terms

Barracuda Networks Software License Agreement Appendix

The GNU General Public License (GPL) Version 2, June 1991
Copyright © 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".
Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.
You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement).

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent

obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF GNU TERMS AND CONDITIONS

Barracuda Networks Products may contain programs that are copyright (c)1995-2005 International Business Machines Corporation and others. All rights reserved. These programs are covered by the following License: "Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation."

Barracuda Networks Products may include programs that are covered by the BSD License: "Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

The names of the authors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE."

Barracuda Networks Products may include the libspf library which is Copyright (c) 2004 James Couzens & Sean Comeau, All rights reserved. It is covered by the following agreement: Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHORS MAKING USE OF THIS LICENSE OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Barracuda Networks Products may contain programs that are Copyright (c) 1998-2003 Carnegie Mellon University. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. The name "Carnegie Mellon University" must not be used to endorse or promote products derived from this software without prior written permission. For permission or any other legal details, please contact Office of Technology Transfer, Carnegie Mellon University, 5000 Forbes Avenue, Pittsburgh, PA 15213-3890 (412) 268-4387, fax: (412) 268-7395, tech-transfer@andrew.cmu.edu . Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by Computing Services at Carnegie Mellon University (http://www.cmu.edu/computing/)." CARNEGIE MELLON UNIVERSITY DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, AND IN NO EVENT SHALL CARNEGIE MELLON UNIVERSITY BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Barracuda Networks Software may include programs that are covered by the Apache License or other Open Source license agreements. The Apache license is re-printed below for you reference. These programs are copyrighted by their authors or other parties, and the authors and copyright holders disclaim any warranty for such programs. Other programs are copyright by Barracuda Networks.

Apache License

Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

> (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and
>
> (b) You must cause any modified files to carry prominent notices stating that You changed the files; and
>
> (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and
>
> (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.
>
> You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including

any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

Barracuda Networks makes available the source code used to build Barracuda products available at source.barracuda.com. This directory includes all the programs that are distributed on the Barracuda products. Obviously not all of these programs are utilized, but since they are distributed on the Barracuda product we are required to make the source code available.